SonicWALL Security Appliances

SonicOS Enhanced 2.5 Administrator's Guide

PART 1: Introduction to SonicOS Enhanced 2.5

Chapter 1: Introduction 1
SonicOS Enhanced 2.5 1
  What's New in SonicOS Enhanced 2.5 1
About this Guide 2
  Organization of this Guide 3
  Guide Conventions 5
SonicWALL Technical Support 6
  SonicWALL Support Solutions 6
More Information on SonicWALL Products 7

Chapter 2: Getting Started 9
  Configuring Your Management Station 9
  Accessing the Management Interface 10
  Troubleshooting 11
  Using the Management Interface 12

PART 2: System

Chapter 3: Viewing Status Information 17
System > Status 17
  Wizards 18
  System Messages 18
  System Information 18
  Latest Alerts 18
  Registration and Security Services 19
  Network Interfaces 22

Chapter 4: Managing SonicWALL Security Services Licenses 23
System > Licenses 23
  Security Services Summary 23
  Manage Security Services Online 24
  Manual Upgrade 25
  Manual Upgrade for Closed Environments 25

Chapter 5: Configuring SonicWALL Security Appliance Administration Settings27
System > Administration 27
  Firewall Name 27
  Administrator Name & Password 28
  Login Security 28
  Web Management Settings 28
  Advanced Management 29
  Enabling SNMP Management 30
  Enable GMS Management 31
  VPN Client Download URL 33

Chapter 6: Configuring Time Settings 35
System > Time 35
  System Time 36
  NTP Settings 36

Chapter 7: Managing SonicWALL Security Appliance Firmware 37
System > Settings 37
Settings 37
Firmware Management 38
SafeMode - Rebooting the SonicWALL Security Appliance. 40
FIPS (PRO 3060/PRO 4060/PRO 5060) 41

Chapter 8: Using Diagnostic Tools & Restarting the SonicWALL Security Appliance 43
System > Diagnostics 43
Diagnostic Tools. 44
System > Restart. 48

PART 3: Network

Chapter 9: Configuring Interfaces 51
Network > Interfaces 51
Setup Wizard 51
Physical Interfaces 51
SonicOS Enhanced Secure Objects 52
Transparent Mode 52
Interface Settings 52
Inteface Traffic Statistics 53
Configuring the LAN/DMZ/Custom Interface (Static) 53
Configuring the LAN/DMZ/Custom Interface (Transparent Mode) 55
Configuring the WLAN Interface. 57
Configuring the WAN Interface. 57
Configuring the Advanced Settings for the WAN Interface 60

Chapter 10:Setting Up WAN Failover and Load Balancing 63
Network > WAN Failover & LB 63
WAN Failover Caveats 63
Setting Up WAN Failover and Load Balancing. 64
WAN Load Balancing Statistics 68

Chapter 11:Configuring Zones 69
Network > Zones 69
How Zones Work 69
Predefined Zones. 70
Security Types 71
Allow Interface Trust. 71
Enabling SonicWALL Security Services on Zones. 71
The Zone Settings Table 72
Adding a New Zone 73
Deleting a Zone 73
Configuring the WLAN Zone 73

Chapter 12:Configuring DNS Settings 77
Network > DNS 77

Chapter 13:Configuring Address Objects . . . 79
Network > Address Objects . . . 79
Types of Address Objects . . . 79
Address Object Groups . . . 80
Creating and Managing Address Objects . . . 80
Default Address Objects and Groups . . . 81
SonicWALL PRO 5060 . . . 81
SonicWALL PRO 4060 . . . 82
SonicWALL PRO 3060 . . . 83
SonicWALL PRO 2040 . . . 84
Adding an Address Object . . . 85
Creating Group Address Objects . . . 85
Public Server Wizard . . . 86

Chapter 14:Configuring Routes . . . 87
Network > Routing . . . 87
Route Advertisement . . . 87
Route Policies . . . 89
Policy Based Routing . . . 89
Route Policies Table . . . 90
A Route Policy Example . . . 90

Chapter 15:Configuring NAT Policies . . . 93
Network > NAT Policies . . . 93
NAT Policies Table . . . 94
NAT Policy Settings Explained . . . 95
NAT Policies Q&A . . . 96
Creating NAT Policies . . . 97

Chapter 16:Managing ARP Traffic . . . 105
Network > ARP . . . 105
Navigating and Sorting the ARP Cache Table Entries . . . 105
Flushing the ARP Cache . . . 106

Chapter 17:Setting Up the DHCP Server . . . 107
Network > DHCP Server . . . 107
Enabling DHCP Server . . . 107
Configuring DHCP Server for Dynamic Ranges . . . 108
Configuring Static DHCP Entries . . . 110
Current DHCP Leases . . . 111

Chapter 18:Using IP Helper . . . 113
Network > IP Helper . . . 113
IP Helper Settings . . . 113
IP Helper Policies . . . 114
Adding an IP Helper Policy . . . 114
Editing an IP Helper Policy . . . 114
Deleting IP Helper Policies . . . 114

Chapter 19:Setting Up Web Proxy Forwarding . . . 115
Network > Web Proxy . . . 115
Configuring Automatic Proxy Forwarding (Web Only) . . . 115
Bypass Proxy Servers Upon Proxy Failure . . . 116

:

Part 4: Wireless

Chapter 20:Managing SonicPoints 119
  - Wireless > SonicPoints 119
  - Before Managing SonicPoints 119
  - SonicPoint Provisioning Profiles 120
    - Configuring a SonicPoint Profile. 120
    - Updating SonicPoint Settings. 123
    - Updating SonicPoint Firmware. 124
    - Automatic Provisioning (SDP & SSPP) 124
    - SonicPoint States. 125

Chapter 21:Viewing Station Status 127
  - Wireless > Station Status 127
    - Event and Statistics Reporting 127

Chapter 22:Using and Configuring IDS 129
  - Wireless > IDS. 129
    - Detecting Wireless Access Points 129
    - Wireless Intrusion Detection Services 129

Part 5: Firewall

Chapter 23:Configuring Access Rules 133
  - Firewall > Access Rules 133
    - Stateful Packet Inspection Default Access Rules Overview. 134
    - Using Bandwidth Management with Access Rules Overview 134
  - Configuration Task List 135
    - Displaying Access Rules with View Styles. 135
    - Configuring Access Rules for a Zone. 136
    - Adding Access Rules 137
    - Editing an Access Rule 138
    - Deleting an Access Rule 138
    - Enabling and Disabling an Access Rule. 139
    - Displaying Access Rule Traffic Statistics 139
  - Access Rule Configuration Examples 139
    - Enabling Ping 139
    - Blocking LAN Access for Specific Services 140
    - Enabling Bandwidth Management on an Access Rule. 140

Chapter 24:Configuring Advanced Access Rule Settings141
  - Firewall > Advanced 141
    - Detection Prevention 142
    - Dynamic Ports 142
    - Source Routed Packets 142
    - TCP Connection Inactivity Timeout 142
    - Access Rule Service Options. 142

Chapter 25:Setting Access Rule Schedules 143
  - Firewall > Schedules 143
    - Schedules. 143
    - Adding a Schedule 144
    - Deleting Schedules 144

Chapter 26:Configuring Firewall Services 145
Firewall > Services 145
Default Services Overview 146
Custom Services Configuration Task List 146
Supported Protocols 146
Adding Custom Services 147
Adding a Custom Services Group 148

Chapter 27:Configuring Multicast Settings 151
Firewall > Multicast 151
Multicast Snooping 152
Multicast Policies 152
IGMP State Table 152
Configuration Example 153

Chapter 28:Configuring VoIP Support 155
Firewall > VoIP 155
VoIP Protocols 155
Configuring the VoIP Settings 156

PART 6: VPN

Chapter 29:Configuring VPN Policies 161
VPN > Settings 161
VPN Policy Wizard 162
VPN Global Settings 163
VPN Policies 163
Currently Active VPN Tunnels 164
Configuring GroupVPN Policies 164
Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone 165
Configuring GroupVPN with IKE using 3rd Party Certificates 168
Exporting a VPN Client Policy 170
Site-to-Site VPN Configurations 171
VPN Planning Sheet for Site-to-Site VPN Policies 171
Creating Site-to-Site VPN Policies 172
Configuring a VPN Policy with IKE using Preshared Secret 174
Configuring a VPN Policy using Manual Key 177
Configuring a VPN Policy with IKE using a Third Party Certificate 181

Chapter 30:Configuring Advanced VPN Settings 185
VPN>Advanced 185
Advanced VPN Settings 185

Chapter 31:Configuring DHCP Over VPN 187
VPN > DHCP over VPN 187
DHCP Relay Mode 187
Configuring the Central Gateway for DHCP Over VPN 187
Configuring DHCP over VPN Remote Gateway 189
Current DHCP over VPN Leases 191

Chapter 32:Configuring L2TP Server 193
VPN > L2TP Server 193
Configuring the L2TP Server 194

Chapter 33:Configuring VPN Certificates 197
VPN>CA Certificates 197
Implementing Certificates for VPN Policies 198
Importing CA Certificates into the SonicWALL Security Appliance 198
Certificate Details 199
Delete This Certificate 199
Certificate Revocation List (CRL) 199
VPN > Local Certificates 200
Importing Certificate with Private Key 200
Certificate Details 201
Delete This Certificate 201
Generating a Certificate Signing Request 201

PART 7: Users

Chapter 34:Managing User Status and Authentication Settings 205
Users>Status 205
User>Settings 206
Authentication Method 206
Configuring RADIUS Authentication 206
Global User Settings 210
Acceptable Use Policy 211

Chapter 35:Managing Local Users and Local Groups213
User > Local Users 213
Viewing Local Users 214
Adding Local Users 214
Editing Local Users 215
Users>Local Groups 215
Creating a Local Group 216

Chapter 36:Managing Guest Services and Guest Accounts 217
Users > Guest Services 217
Global Guest Settings 218
Guest Profiles 218
Users > Guest Accounts 219
Adding Guest Accounts 219
Enabling Guest Accounts 221
Enabling Auto-prune for Guest Accounts 222
Printing Account Details. 222
Users > Guest Status 223
Logging Accounts off the Appliance 223

PART 8: Hardware Failover

Chapter 37:Setting Up Hardware Failover 227
Hardware Failover > Settings 227
How Hardware Failover Works. 227
Before Configuring Hardware Failover 228
Configuring Hardware Failover. 231
Sychronizing Firmware 233
Monitoring Links 233
Hardware Failover Status 233

PART 9: Security Services

Chapter 38:Managing Security Services 237
Security Services>Summary 237
mySonicWALL.com. 237
Security Services Summary 238

Chapter 39:Configuring SonicWALL Content Filter 241
Security Services>Content Filter 241
SonicWALL Content Filtering Service. 241
Content Filter Status 242
Content Filter Type 243
Restrict Web Features 244
Trusted Domains. 244
Message to Display when Blocking 245
Configuring SonicWALL Filter Properties 245
Custom List. 245
Consent. 246
Mandatory Filtered IP Addresses 247

Chapter 40:Activating SonicWALL Network Anti-Virus. 249
Security Services>Anti-Virus 249
Activating SonicWALL Network Anti-Virus 250
Activating a SonicWALL Network Anti-Virus FREE TRIAL 250
Security Services>E-Mail Filter 251

Chapter 41:Activating Intrusion Prevention Service. 253
Security Services > Intrusion Prevention 253
SonicWALL IPS Features 253
SonicWALL Deep Packet Inspection 254
How SonicWALL's Deep Packet Inspection Works 255
SonicWALL IPS Terminology 255
SonicWALL IPS Activation 256
Activating SonicWALL IPS 257
Activating the SonicWALL IPS FREE TRIAL 257

PART 10: Log

Chapter 42:Managing Log Events. 261
Log > View 261
Log View Table 262
Refresh 262
Clear Log 262
Export Log. 263
E-mail Log. 263
Log Event Messages 263

Chapter 43:Configuring Log Categories 291
Log > Categories 291
Log Priority 292
Log Categories 292

Chapter 44:Configuring Syslog Settings 295
Log > Syslog 295
Syslog Settings. 296
Syslog Servers 296

Chapter 45:Configuring Log Automation. 297
Log > Automation 297
E-mail Log Automation 297
Mail Server Settings 298

Chapter 46:Generating Log Reports 299
Log > Reports 299
Data Collection 300
View Data 300

Chapter 47:Activating and Enabling SonicWALL ViewPoint 301
Log > ViewPoint 301
Activating ViewPoint 302
Enabling ViewPoint Settings 303

PART 11: Wizards

Chapter 48:Configuring Internet Connectivity Using the Setup Wizard 307
Internet Connectivity Using the Setup Wizard 307
Configuring a Static IP Address with NAT Enabled 307
Configuring DHCP Networking Mode 312
Configuring NAT Enabled with PPPoE. 317
Configuring PPTP Network Mode 322

Chapter 49:Configuring a Public Server with the Wizard 329
Create a Server with the Public Server Wizard 329

Chapter 50:Configuring VPN Policies with the VPN Policy Wizard 335
Configuring GroupVPN using the VPN Policy Wizard 335
Using the VPN Policy Wizard 335
Connecting the Global VPN Clients 338
Configuring a Site-to-Site VPN using the VPN Wizard 339
Using the VPN Wizard to Configure Preshared Secret 339

Chapter 51:Index. 343

Preface

Copyright Notice

© 2004 SonicWALL, Inc. All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

SonicWALL is a registered trademark of SonicWALL, Inc.

Other product and company names mentioned herein can be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions subject to change without notice.

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY

EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Current Documentation

Check the SonicWALL documentation Web site for that latest versions of this manual and all other SonicWALL product documentation.

http://www.sonicwall.com/services/documentation.html

PART

1

Introduction to SonicOS Enhanced 2.5

:

CHAPTER 1

Introduction

SonicOS Enhanced 2.5

SonicOS Enhanced is the most powerful SonicOS operating system designed for the latest generation of SonicWALL security appliances. SonicOS Enhanced 2.5 is standard on the SonicWALL PRO 4060 and PRO 5060 and available as an upgrade on the SonicWALL TZ170 Series, PRO 2040, and PRO 3060.

What's New in SonicOS Enhanced 2.5

Built on the SonicOS architecture, this operating system features multiple network interfaces and zones, WAN ISP failover and load balancing, policy-based NAT, object-based management, a multi-level administrator GUI, and enhanced VPN functionality. SonicOS Enhanced 2.5 builds on these features with powerful new capabilities and industry-leading technologies.

- **Updated Configuration Wizard**: SonicOS Enhanced 2.5 includes an new configuration wizard that includes three configuration wizards: Setup Wizard, Public Server Wizard, and VPN Policy Wizard to provide you with a quick, easy, and comprehensive configuration of the SonicWALL security appliance for common deployment scenarios.
- **Enhanced VoIP Support**: SonicOS Enhanced 2.5 adds comprehensive support for third-party VoIP equipment, including products from Cisco, Mitel, Pingtel, Grandstream, Polycom, D-Link, Pulver, Apple iChat, and softphones from Yahoo, Microsoft, Ubiquity, and OpenPhone. SonicOS Enhanced 2.5 adds the ability to handle SIP, RTSP, H.323v1, H.323v2, H.323v3, H.323v4, H.323 gatekeepers, and LDAP ILS support. The internal DHCP Server capability in SonicOS Enhanced 2.5 allows Cisco CallManager addressing information into the DHCP scope information, so that Cisco phones can receive addresses when they issue a DHVCP request on the network.
- **Hardware Failover Enhancements**: SonicOS Enhanced 2.5 includes a number of useful enhancements to hardware failover, including the ability to automatically synchronize the firmware between the Primary and Backup SonicWALL security appliances, and the ability to load new firmware versions on to both devices simultaneously from the Primary SonicWALL security appliance. You can also specify logical monitoring addresses for each interface.
- **Flexible VPN Termination**: SonicOS Enhanced 2.5 includes the ability to terminate incoming site-to-site VPN connections on any interface. This feature is useful in situations where untrusted transit networks terminate on internal interfaces; an example of this might be a router sitting on a DMZ Zone/Interface with an untrusted Frame Relay network connecting the router to a business partner. Using the flexible VPN termination feature, you are able to run a VPN connection across the Frame Relay connection and know the Frame Relay provider cannot see the traffic.

- **Multiple GroupVPN Policies**: SonicOS Enhanced 2.5 allows you to create separate, customized GroupVPN policies for each Zone, and SonicWALL Global VPN Client connections can terminate on any interface.
- **Wireless Extensions**: SonicOS Enhanced 2.5 includes the ability to terminate wireless clients using SonicWALL SonicPoint, and incorporating wireless features such as wireless guest services (WGS), secure wireless roaming, using SonicWALL's Global VPN Client, and rogue access point detection. SonicOS Enhanced 2.5 allows you to manage SonicWALL SonicPoints for secure wireless networking behind the firewall.
- **Full Stateful IGMP Multicast Support**: SonicOS Enhanced 2.5 includes the ability to track and allow/deny multicast traffic, with support for IGMPv1, IGMPv2, and IGMPv3. Multicast can be enabled or disabled on a per-interface and per-VPN policy basis.
- **Inbound Bandwidth Management**: SonicOS Enhanced 2.5 adds the ability to perform ingress and egress bandwidth management for traffic passing in and out of the WAN interfaces on a per-rule basis. Ingress bandwidth management uses rate-limiting via delayed ACKs for TCP traffic, drops over-limit packets for connectionless UDP traffic. For both methods, you specify the maximum upstream and downstream throughput for each WAN interface, and on a per-rule basis, set the priority level of the traffic, the guaranteed percentage of bandwidth for that rule, and the maximum (i.e. burstable) bandwidth for that rule.
- **Transparent Mode Suppor**t: SonicOS Enhanced 2.5 includes the ability to bridge WAN-side IP addresses/subnets onto an internal interface, including the LAN Zone interface. This feature is useful in network environments where it is not possible to renumber internal systems to a private addressing scheme and perform NAT at the SonicWALL security appliance, or in "drop-in" situations where the SonicWALL security appliance is used primarily as an IPS (Intrusion Prevention Service) or CFS (Content Filtering Service) appliance.
- **Expanded IP Protocol Support**: SonicOS Enhanced 2.5 supports additional IP types (IGRE, ESP, AH, EIGRP, OSPF, PIMSM, L2TP) as well as specify ICMP/IGMP subtypes when creating customized service objects, across the firewall and through VPN connections.
- **Policy Based Routing (PBR)** - SonicOS Enhanced 2.5 allows you to create extended static routes that match against source, service, and destination. This feature, for example, can be used to steer traffic matching the route policies out a specific WAN. It also supports metrics, so high-cost static route entries can be used in case dynamically received route entries fail.
- **Expanded Logging**: SonicOS Enhanced 2.5 includes additional logging capabilities to provide expanded flexibility. You can export the log into plain text or CSV values. Logging categories are dramatically expanded, the logs conform to Syslog severity levels so you can set the SonicWALL security appliance to only log alerts and messages of specified levels, and you can independently specify which categories are logged to the internal log. When directing logs to external Syslog servers, you can rate-limit the messages based on events per second, or maximum bytes per second, so that external Syslog servers do not get overwhelmed. The SonicWALL security appliance also has the ability to do "POP before SMTP" in order to e-mail logs and alerts to SMTP mail servers that require a successful POP3 authentication before e-mail is sent through them.

About this Guide

Welcome to the *SonicWALL SonicOS Enhanced 2.5 Administrator's Guide*. This manual provides the information you need to successfully activate, configure, and administer SonicOS Enhanced 2.5 for the SonicWALL TZ170, PRO 2040, PRO 3060, PRO 4060, and PRO 5060 Internet Security Appliances.

Note: *Always check <http//:www.sonicwall.com/services/documentation.html> for the latest version of this manual as well as other SonicWALL products and services documentation.*

Organization of this Guide

The SonicOS Enhanced 2.5 Administrator's Guide organization is structured into the following parts that follow the SonicWALL Web Management Interface structure. Within these parts, individual chapters correspond to Management Interface layout.

Part 1 Introduction

This part provides an overview of new SonicWALL SonicOS Enhanced features, guide conventions, and instructions for connecting a management station to the SonicWALL security appliance to access the SonicWALL Management Interface.

Part 2 System

This part covers a variety SonicWALL security appliance controls for managing system status information, registering the SonicWALL security appliance, activating and managing SonicWALL Security Services licenses, configuring SonicWALL security appliance local and remote management options, managing firmware versions and preferences, and using included diagnostics tools for troubleshooting.

Part 3 Network

This part covers configuring the SonicWALL security appliance for your network environment. The **Network** section of the SonicWALL Management Interface includes:

- **Interfaces** - configure logical interfaces for connectivity.
- **WAN Failover and Load Balancing** - configure one of the user-defined interfaces to act as a secondary WAN port for backup or load balancing.
- **Zones** - configure security zones on your network.
- **DNS** - set up DNS servers for name resolution.
- **Address Objects** - configure host, network, and address range objects.
- **Routing** - view the **Route Table**, **ARP Cache** and configure static and dynamic routing by interface.
- **NAT Policies** - create NAT policies including One-to-One NAT, Many-to-One NAT, Many-to-Many NAT, or One-to-Many NAT.
- **ARP** - view the ARP settings and clear the ARP cache as well as configure ARP cache time.
- **DHCP Server -** configure the SonicWALL as a DHCP Server on your network to dynamically assign IP addresses to computers on your LAN or DMZ zones.
- **IP Helper** - configure the SonicWALL to forward DHCP requests originating from the interfaces on the SonicWALL to a centralized server on behalf of the requesting client.
- **Web Proxy** - configure the SonicWALL to automatically forward all Web proxy requests to a network proxy server.

Part 4 Wireless

The part covers the configuration of the SonicWALL security appliance for provisioning and managing SonicWALL SonicPoints as part of a SonicWALL Distributed Wireless Solution.

Cross Reference: *For more information on SonicWALL's Distributed Wireless Solution, go to http://www.sonicwall.com/products/wirelesssolutions.html.*

Part 5 Firewall

This part covers tools for managing how the SonicWALL security appliance handles traffic through the the firewall, including Multicast and VoIP traffic.

Part 6 VPN

This part covers how to create VPN policies on the SonicWALL security appliance to support SonicWALL Global VPN Clients as well as creating site-to-site VPN policies for connecting offices running SonicWALL security appliances.

Part 7 Users

This part covers how to configure the SonicWALL security appliance for user level authentication as well as manage guest services for managed SonicPoints.

Part 8 Hardware Failover

This part provides configuration instructions for setting a SonicWALL high availability pair for maintaining secure, mission-critical connectivity.

Part 9 Security Services

This part includes an overview of available SonicWALL Security Services as well as instructions for activating the service, including FREE trials. These subscription-based services include SonicWALL Content Filtering Service, SonicWALL Instrusion Prevention Service, SonicWALL Network Anti-Virus, and well as other services.

➲ **Cross Reference:** *For more information on SonicWALL Security Services, go to <http//:www.sonicwall.com.*

Part 10 Log

This part covers managing the SonicWALL security appliance’s enhanced logging, alerting, and reporting features. The SonicWALL security appliance’s logging features provide a comprehensive set of log categories for monitoring security and network activities.

Part 11 Wizards

This part walks you through using the SonicWALL Configuration Wizards for configuring the SonicWALL security appliance for LAN to WAN (Internet) connectivity, settings up public servers for Internet connectivity behind the firewall, and setting GroupVPN and site-to-site VPN policies for establishing VPN connections for remote SonicWALL Global VPN Client users or remote offices with a SonicWALL security appliance for LAN to LAN connections.

The SonicWALL Configuration Wizards in SonicOS Enhanced 2.5 or higher include:

- The **Setup Wizard** takes you step by step through network configuration for Internet connectivity. There are four types of network connectivity available: Static IP, DHCP, PPPoE, and PPTP.
- The **Public Server Wizard** takes you step by step through adding a server to your network, such as a mail server or a web server. The wizard automates much of the configuration you need to establish security and access for the server.
- The **VPN Policy Wizard** steps you through the configuration of Group VPNs and site-to-site VPNs.

Guide Conventions

The following Conventions used in this guide are as follows:

Convention	**Use**
Bold	Highlights items you can select on the SonicWALL Management Interface.
Italic	Highlights a value to enter into a field. For example, “type *192.168.168.168* in the **IP Address** field.”
Menu Item > Menu Item	Indicates a multiple step Management Interface menu choice. For example, “**Security Services>Content Filter** means select Security Services, then select Content Filter.

Icons Used in this Manual

These special messages refer to noteworthy information, and include a symbol for quick identification:

▲ **Alert:** *Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWALL.*

✓ **Tip:** *Useful information about security features and configurations on your SonicWALL.*

✎ **Note:** *Important information on a feature that requires callout for special attention.*

➡ **Cross Reference:** *Provides a pointer to related information in the Administrator’s Guide or other resources.*

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <*http://www.sonicwall.com/services/support.html*>. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

To contact SonicWALL telephone support, see the telephone numbers listed below:

North America Telephone Support

U.S./Canada - 888.777.1476 or +1 408.752.7819

International Telephone Support

Australia - + 1800.35.1642

Austria - + 43(0)820.400.105

EMEA - +31(0)411.617.810

France - + 33(0)1.4933.7414

Germany - + 49(0)1805.0800.22

Hong Kong - + 1.800.93.0997

India - + 8026556828

Italy - +39.02.7541.9803

Japan - + 81(0)3.5460.5356

New Zealand - + 0800.446489

Singapore - + 800.110.1441

Spain - + 34(0)9137.53035

Switzerland - +41.1.308.3.977

UK - +44(0)1344.668.484

Note: *Please visit <http://www.sonicwall.com/services/contact.html> for the latest technical support telephone numbers.*

SonicWALL Support Solutions

SonicWALL's powerful security solutions give unprecedented protection from the risks of Internet attacks. SonicWALL's comprehensive support services protect your network security investment and offer the support you need - when you need it.

Note: *For complete information on SonicWALL Support Solutions, please visit <http://www.sonicwall.com/services/support.html.*

Knowledge Base

All SonicWALL customers have immediate, 24X7 access to our state-of-the-art electronic support tools. Power searching technologies on our Web site allow customers to locate information quickly and easily from our robust collection of technical information - including manuals, product specifications, operating instructions, FAQs, Web pages, and known solutions to common customer questions and challenges.

Internet Security Expertise

Technical Support is only as good as the people providing it to you. SonicWALL support professionals are Certified Internet Security Administrators with years of experience in networking and Internet security. They are also supported by the best in class tools and processes that ensure a quick and accurate solution to your problem.

SonicWALL Support Programs

SonicWALL offers a variety of support programs designed to get the support you need when you need it. For more information on SonicWALL Support Services, please visit <http://www.sonicwall.com/products/supportservices.html.

Warranty Support - North America and International

SonicWALL products are recognized as extremely reliable as well as easy to configure, install, and manage. SonicWALL Warranty Support enhances these features with

- 1 year, factory replacement for defective hardware
- 90 days of advisory support for installation and configuration assistance during local business hours
- 90 days of software and firmware updates
- Access to SonicWALL's electronic support and Knowledge Base system.

More Information on SonicWALL Products

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

Web: http://www.sonicwall.com
E-mail: sales@sonicwall.com
Phone: (408) 745-9600
Fax: (408) 745-9300

CHAPTER

2

Getting Started

Configuring Your Management Station

Your SonicWALL security appliance is configured with the default IP address of 192.168.168.168. This IP address is used to initially access the Management Interface of the SonicWALL security appliance.

➲ **Cross Reference:** *For instructions on setting up your SonicWALL security appliance, see the SonicWALL Quick Start Guide.*

To access the Management Interface for the first time, you must configure your computer with an IP address in the same network range as the SonicWALL security appliance. Follow the instructions below for your operating system:

Windows XP

- Right-click **My Network Place** and select **Properties**.
- Right-click on the **Local Area Connection** icon and select **Properties**.
- Open the **Local Area Connection Properties** window.
- Double-click **Internet Protocol (TCP/IP)** to open the **Internet Protocol (TCP/IP) Properties** window.
- Select **Use the following IP address** and type 192.168.168.200 in the **IP address** field.
- Enter 255.255.255.0 in the **Subnet Mask** field.
- Enter the DNS IP address in the **Preferred DNS Server** field. If you have more than one address, type the second one in the **Alternate DNS server** field.
- Click **OK** for the settings to take effect on the computer.

Windows 2000

1. From your Windows task bar, click **Start**.
2. Then click **Settings**.
3. Click **Network and Dial-up Connections**.
4. Double-click the network icon to open the connection window.
5. Click **Properties**.
6. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
7. Select **Use the following IP address**.
8. Enter 192.168.168.200 in the **IP address** field.

9. Enter 255.255.255.0 in the **Subnet** field.
10. If you have a DNS Server IP address from your ISP, enter it in the **Preferred DNS Server** field.
11. Click **OK**.

Windows NT

1. From the **Start** list, highlight **Settings** and then select **Control Panel**.
2. Double-click the **Network** icon in the **Control Panel** window.
3. Double-click **TCP/IP** in the **TCP/IP Properties** window.
4. Select **Specify an IP Address**.
5. Enter 192.168.168.200 in the **IP Address** field.
6. Enter 255.255.255.0 in the **Subnet Mask** field.
7. Click **DNS** at the top of the window.
8. Type the DNS IP address in the **Preferred DNS Server** field. If you have more than one address, enter the second one in the **Alternate DNS server** field.
9. Click **OK**, and then click **OK** again.
10. Restart the computer.

Windows 98

1. From the **Start** list, highlight **Settings** and then select **Control Panel**. Double-click the **Network** icon in the **Control Panel** window.
2. Double-click **TCP/IP** in the **TCP/IP Properties** window.
3. Select **Specify an IP Address**.
4. Enter 192.168.168.200 in the **IP Address** field.
5. Enter 255.255.255.0 in the **Subnet Mask** field.
6. Click **DNS Configuration**.
7. Type the DNS IP address in the **Preferred DNS Server** field. If you have more than one address, type the second one in the **Alternate DNS server** field.
8. Click **OK**, and then click **OK** again.
9. Restart the computer.

Accessing the Management Interface

To access the SonicWALL Management Interface, you need to configure the Management Station TCP/IP settings in order to initially contact the SonicWALL. A computer used to manage the SonicWALL is referred to as the “Management Station.” Any computer on the same network as the SonicWALL can be used to access the management interface.

MD5 authentication is used to secure communications between your Management Station and the SonicWALL Web Management Interface. MD5 Authentication prevents unauthorized users from detecting and stealing the SonicWALL password as it is sent over your network.

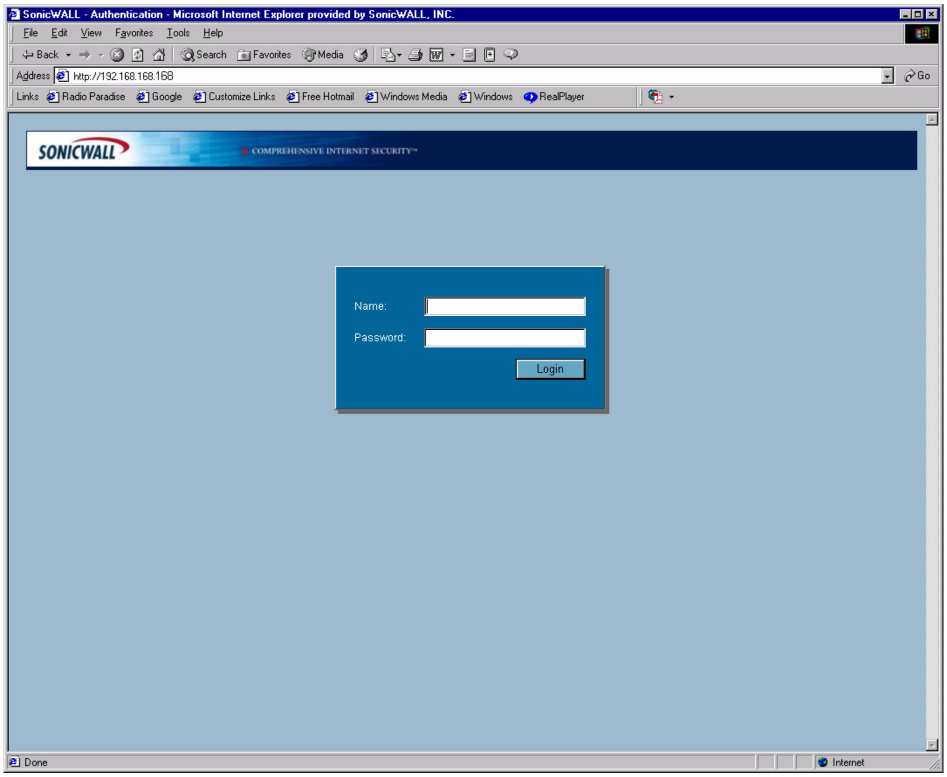
The Web browser used to access the management interface must be Java-enabled and support HTTP uploads in order to fully manage the SonicWALL. If your Web browser does not support these functions, certain features such as uploading firmware and saved preferences files are not available.

▲ **Alert:** *Please allow enough time for the SonicWALL security appliance to power up completely before attempting to log into the Management Interface. It takes approximately one minute for the SonicWALL security appliance to cycle completely. When the **Test** light is no longer lit, the SonicWALL security appliance is ready for configuration.*

Alert: *Because you are temporarily disconnected from the Internet, you may receive an error message when your Web browser first opens. This does not affect your installation process. Continue with the steps below.*

To begin the configuration of your SonicWALL security appliance, you must log into the SonicWALL security appliance using a Web browser and the SonicWALL security appliance default LAN IP address, 192.168.168.168. Follow the instructions below:

1. Launch your Web browser.
2. Enter 192.168.168.168 in the **Location** or **Address** field.
3. The first time you log into the SonicWALL Management Interface, the **Setup Wizard** is automatically displayed for configuring your WAN (Internet) and LAN setup.


SonicWALL - Authentication - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.168
Go
Links Radio Paradise Google Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
Name:
Password:
Login
Done
Internet

Cross Reference: *See Chapter 49 Configuring Internet Connecitivity using the* ***Setup Wizard****.*

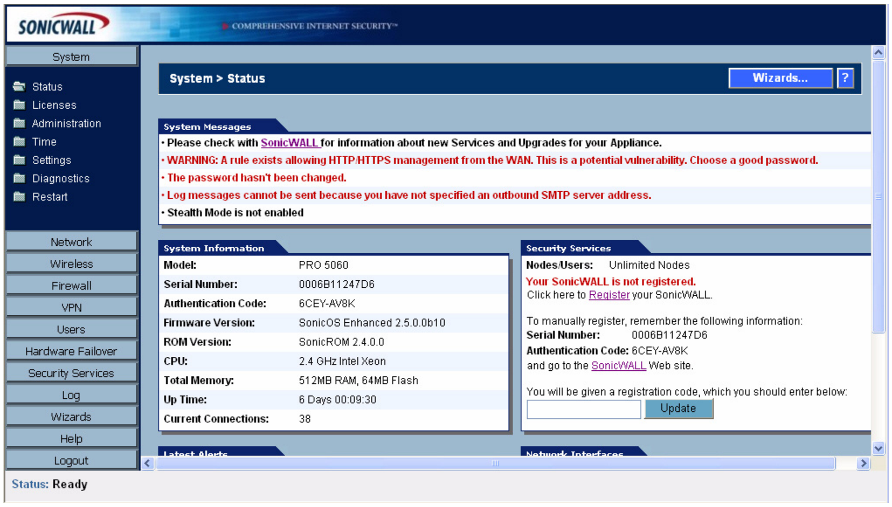
Troubleshooting

If you cannot connect to the SonicWALL security appliance, check the following:

- Did you correctly enter the SonicWALL security appliance default LAN IP address in your browser window?
- Is the SonicWALL security appliance connected to the same network as your computer?
- Have you changed the TCP/IP network settings on your computer?
- Try pinging the 192.168.168.168 LAN IP address of the SonicWALL security appliance from your computer. It should reply, assuming that you are using the correct TCP/IP network settings and have a good ethernet connection. If it does reply, try again with the web browser to 192.168.168.168.

Using the Management Interface

The SonicWALL's Web Management Interface provides a easy-to-use graphical interface for configuring your SonicWALL. SonicWALL management functions are performed through a Web browser.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Status
Wizards...
?
Update
Latest Alerts
Network Interfaces

System Messages

- Please check with SonicWALL for information about new Services and Upgrades for your Appliance.
- WARNING: A rule exists allowing HTTP/HTTPS management from the WAN. This is a potential vulnerability. Choose a good password.
- The password hasn't been changed.
- Log messages cannot be sent because you have not specified an outbound SMTP server address.
- Stealth Mode is not enabled

System Information

Model:	PRO 5060
Serial Number:	0006B11247D6
Authentication Code:	6CEY-AV8K
Firmware Version:	SonicOS Enhanced 2.5.0.0b10
ROM Version:	SonicROM 2.4.0.0
CPU:	2.4 GHz Intel Xeon
Total Memory:	512MB RAM, 64MB Flash
Up Time:	6 Days 00:09:30
Current Connections:	38

Security Services

Nodes/Users: Unlimited Nodes

Your SonicWALL is not registered.
Click here to Register your SonicWALL.

To manually register, remember the following information:
Serial Number: 0006B11247D6
Authentication Code: 6CEY-AV8K
and go to the SonicWALL Web site.

You will be given a registration code, which you should enter below:

Status: Ready

✓ **Tip:** *Microsoft Internet Explorer 5.0 or higher, or, Netscape Navigator 4.5 or higher are two recommended Web browsers.*

Navigating the Management Interface

Navigating the SonicWALL Management Interface includes a hierarchy of menu buttons on the navigation bar (left side of window). The SonicOS Enhanced menu buttons on the navigation bar include:

- System
- Network
- Wireless
- Firewall
- VPN
- Users
- Hardware Failover
- Security Services
- Log
- Wizards
- Help
- Logout

When you click a menu button, related management functions are displayed as submenu items in the navigation bar. To navigate to a submenu page, click the link. When you click a menu button, the first submenu item page is displayed.

Applying Changes

Click the **Apply** button at the top right corner of the SonicWALL Management Interface to save any configuration changes you made on the page.

If the settings are contained in a secondary window within the Management Interface, when you click **OK**, the settings are automatically applied to the SonicWALL.

Getting Help

Each SonicWALL includes Web-based online help available from the Management Interface. Clicking the question mark **?** button on the top right corner of every page accesses the context-sensitive help for the page.

▲ **Alert:** *SonicWALL online help requires Internet connectivity.*

Logging Out

The **Logout** button at the bottom of the menu bar terminates the Management Interface session and displays the Login page.

PART

2

System

:

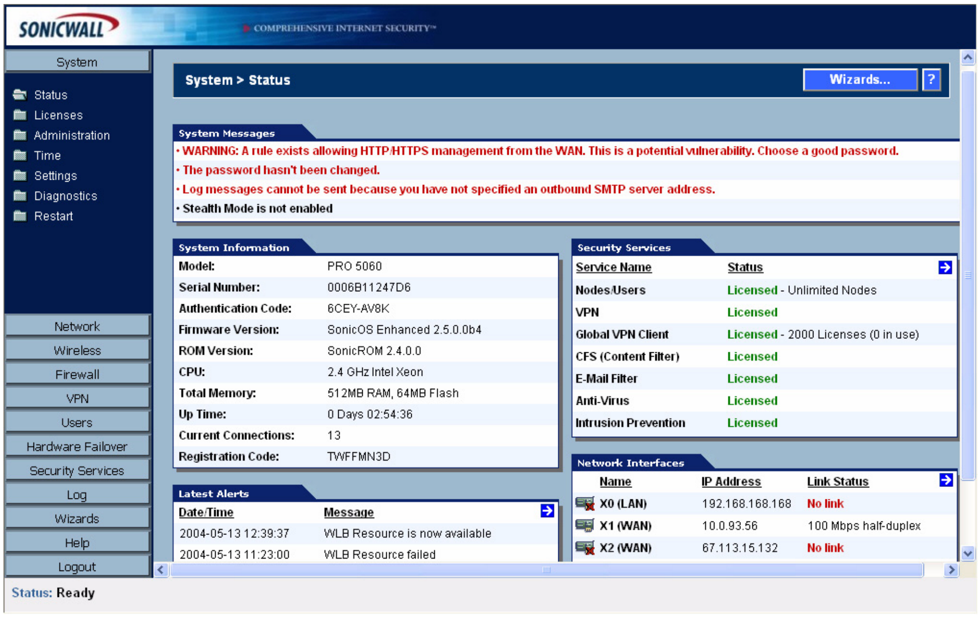
CHAPTER

3

Viewing Status Information

System > Status

The **System>Status** page provides a comprehensive collection of information and links to help you manage your SonicWALL security appliance and SonicWALL Security Services licenses. It includes status information about your SonicWALL security appliance organized into five sections: **System Messages, System Information, Security Services, Latest Alerts,** and **Network Interfaces** as well as the **Wizards** button for accessing the **SonicWALL Configuration Wizard**.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Status
Wizards...
?
Status: Ready

System Messages

- WARNING: A rule exists allowing HTTP/HTTPS management from the WAN. This is a potential vulnerability. Choose a good password.
- The password hasn't been changed.
- Log messages cannot be sent because you have not specified an outbound SMTP server address.
- Stealth Mode is not enabled

System Information

Model:	PRO 5060
Serial Number:	0006B11247D6
Authentication Code:	6CEY-AV8K
Firmware Version:	SonicOS Enhanced 2.5.0.0b4
ROM Version:	SonicROM 2.4.0.0
CPU:	2.4 GHz Intel Xeon
Total Memory:	512MB RAM, 64MB Flash
Up Time:	0 Days 02:54:36
Current Connections:	13
Registration Code:	TWFFMN3D

Security Services

Service Name	Status
Nodes/Users	Licensed - Unlimited Nodes
VPN	Licensed
Global VPN Client	Licensed - 2000 Licenses (0 in use)
CFS (Content Filter)	Licensed
E-Mail Filter	Licensed
Anti-Virus	Licensed
Intrusion Prevention	Licensed

Latest Alerts

Date/Time	Message
2004-05-13 12:39:37	WLB Resource is now available
2004-05-13 11:23:00	WLB Resource failed

Network Interfaces

Name	IP Address	Link Status
X0 (LAN)	192.168.168.168	No link
X1 (WAN)	10.0.93.56	100 Mbps half-duplex
X2 (WAN)	67.113.15.132	No link

Wizards

The **Wizards** button on the **System>Status** page provides access to the **SonicWALL Configuration Wizard**, which allows you to easily configure the SonicWALL security appliance using the following sub-wizards:

- **Setup Wizard** - This wizard helps you quickly configure the SonicWALL security appliance to secure your Internet (WAN) and LAN connections.
- **Public Server Wizard** - This wizard helps you quickly configure the SonicWALL security appliance to provide public access to an internal server, such as a Web or E-mail server.
- **VPN Wizard** - This wizard helps you create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept VPN connections from SonicWALL Global VPN Clients.

Cross Reference: *For more information on using the SonicWALL Configuration Wizard, see Part 11 Wizards.*

System Messages

Any information considered relating to possible problems with configurations on the SonicWALL security appliance such as password, log messages, as well as notifications of SonicWALL Security Services offers, new firmware notifications, and upcoming Security Service s expirations are displayed in the **System Messages** section.

System Information

The following information is displayed in this section:

- **Model** - type of SonicWALL security appliance product
- **Serial Number** - also the MAC address of the SonicWALL security appliance
- **Authentication Code** - the alphanumeric code used to authenticate the SonicWALL security appliance on the registration database at <https://www.mysonicwall.com>.
- **Firmware Version** - the firmware version loaded on the SonicWALL security appliance.
- **ROM Version** - indicates the ROM version.
- **CPU** - displays the type and speed of the SonicWALL security appliance processor.
- **Total Memory** - indicates the amount of RAM and flash memory.
- **Up Time** - the length of time, in days, hours, and seconds the SonicWALL security appliance is active.
- **Current Connections** - the number of network connections currently existing on the SonicWALL security appliance.
- **Registration Code** - the registration code is generated when your SonicWALL security appliance is registered at <http://www.mysonicwall.com>.

Latest Alerts

Any messages relating to system errors or attacks are displayed in this section. Attack messages include AV Alerts, forbidden e-mail attachments, fraudulent certificates, etc. System errors include WAN IP changed and encryption errors. Clicking the blue arrow displays the **Log>Log View** page.

Cross Reference: *For more information on SonicWALL security appliance logging, see Part 10 Log.*

Registration and Security Services

Once you've established your Internet connection, you can register your security appliance at mySonicWALL.com as well as activate SonicWALL Security Services. Any bundled services included with your SonicWALL security appliance are automatically activated when your register.

You need a mySonicWALL.com account to register your security appliance or activate SonicWALL Security Services. You can create a mySonicWALL.com account directly from the SonicWALL Management Interface. If your security appliance is connected to the Internet, and you have a mySonicWALL.com account, you can register the security appliance and activate SonicWALL Security Services directly from the Management Interface.

Registering Your SonicWALL Security Appliance

If your security appliance is not registered, the following message is displayed in the **Security Services** folder on the **System>Status** page in the SonicWALL Management Interface: **Your SonicWALL is not registered. Click here to Register your SonicWALL Security Appliance**.

You can also manually register your security appliance at the www.mySonicWALL.com site by using the **Serial Number** and **Authentication Code** displayed in the **Security Services** section. Click the **SonicWALL** link to access your mySonicWALL.com account. You will be given a registration code after you have registered your security appliance. Enter the registration code in the field below the **You will be given a registration code, which you should enter below** heading, then click **Update**.

The following sections explain how to create a mySonicWALL.com account from the SonicWALL Management Interface, if you don't have an account, and how to register your security appliance directly from the Management Interface.

mySonicWALL.com

mySonicWALL.com delivers a convenient, one-stop resource for registration, activation, and management of your SonicWALL products and services. Your mySonicWALL.com account provides a single profile to do the following:

- Register your SonicWALL security appliances
- Purchase/Activate SonicWALL Security Services and Upgrades
- Receive SonicWALL firmware and security service updates and alerts
- Manage (change or delete) your SonicWALL security services
- Access SonicWALL Technical Support

Creating a mySonicWALL.com account is easy and FREE. Simply complete an online registration form. Once your account is created, you can register SonicWALL security appliance and activate SonicWALL Security Services associated with the security appliance.

Your mySonicWALL.com account is accessible from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information. You can also access mySonicWALL.com license and registration services directly from the SonicWALL management interface for increased ease of use and simplified services activation.

✓ **Tip:** *For more information on mySonicWALL.com, access the online help available at https://www.mysonicwall.com.*

Note: *mySonicWALL.com registration information is not sold or shared with any other company.*

Creating Your mySonicWALL.com Account

If you already have a mySonicWALL.com account, skip this section. To create a mySonicWALL.com account from the SonicWALL Management Interface, follow these steps:

In the **Security Services** folder on the **System>Status** page in the SonicWALL Management Interface, click the here link in **Your security appliance is not registered. Click here to Register your security appliance**. The **mySonicWALL.com Login** page is displayed.

1 Click the **here** link in **If you do not have a mySonicWALL account, please click here to create one**. The mySonicWALL.com account form is displayed.

2 Enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an * are required fields.

▲ **Alert:** *Remember your username and password to access your mySonicWALL.com account.*

3 Click **Submit** after completing the mySonicWALL.com account form.

4 Review your account information. If the information is correct, click **OK**. You will receive a subscription code by e-mail from SonicWALL. This code is required to complete the activation of your new account.

▲ **Alert:** *Your new account must be activated with the subscription code within 72 hours of receiving the code.*

5 After you receive your subscription code, in the **Security Services** folder on the **System>Status** page in the SonicWALL Management Interface, click the here link in **Your SonicWALL is not registered. Click here to Register your SonicWALL**.

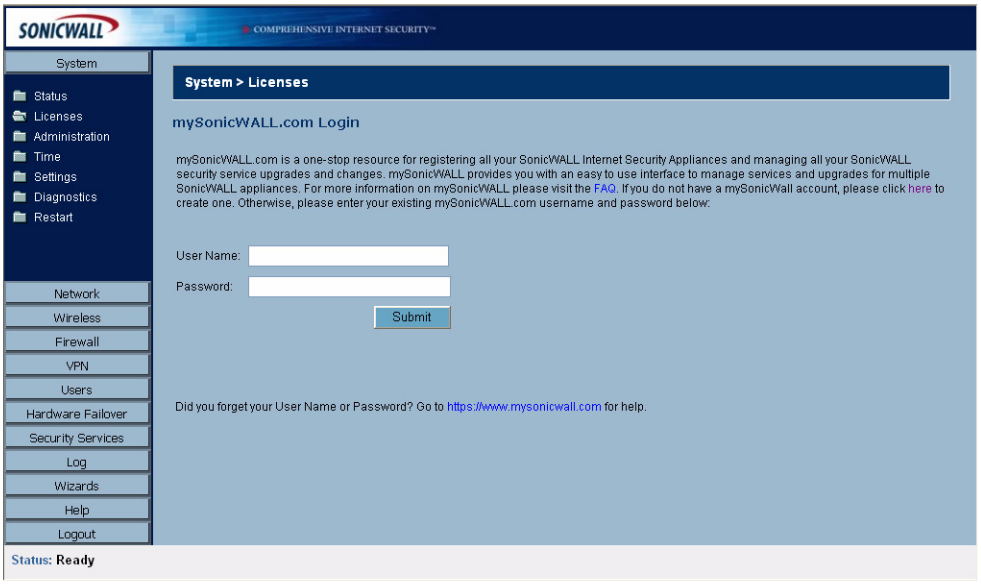
6 In the **mySonicWALL.com Login** page, enter your mySonicWALL.com account username and password, and click **Submit**. You are prompted for the subscription code.

7 Enter your subscription code and click **Submit**. Your mySonicWALL.com account is activated.

Registering the SonicWALL Security Appliance from the Management Interface

If you have a mySonicWALL.com account, follow these steps to register your SonicWALL security appliance:

1. Click the **here** link to automatically register your SonicWALL security appliance. The **mySonicWALL.com Login** page is displayed.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Licenses
Submit

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall account, please click here to create one. Otherwise, please enter your existing mySonicWALL.com username and password below:

User Name:

Password:

Did you forget your User Name or Password? Go to https://www.mysonicwall.com for help.

Status: Ready

2. Type your mySonicWALL.com username and password in the **User Name** and **Password** fields and click **Submit**.
3. Type in a "friendly name" for your SonicWALL security appliance in the **Friendly Name** field. A friendly name is used to help identify your SonicWALL security appliance, such as its location.
4. Click **Submit**. Your SonicWALL security appliance is now registered.

▲ **Alert:** *Make sure the DNS and Time settings on your security appliance are correct when you register the device.*

Security Services

If your SonicWALL security appliance is registered, the **Security Services** section provides a list of currently **Licensed** SonicWALL Security Services and the number of licenses available and in use. Clicking the blue icon displays the **System>Licenses** page in the SonicWALL Web Management Interface. SonicWALL Security Services and SonicWALL security appliance registration is managed by mySonicWALL.com.

➲ **Cross Reference:** *For more information on SonicWALL Security Services, see Part 9 Security Services.*

Network Interfaces

Network Interfaces displays information about the interfaces for your SonicWALL security appliance. Clicking the blue arrow displays the **Network>Settings** page for configuring your **Network** settings. The available interfaces displayed in the Network Interfaces section depends on the SonicWALL security appliance model.

SonicWALL PRO 2040

- **X0) LAN** - IP address and network speed.
- **(X1) WAN** - IP address, network speed and devices connected to the WAN interface.
- **X2** - **X3** - user-defined interfaces.

SonicWALL PRO 3060/PRO 4060

- **(X0) LAN** - IP address and network speed.
- **(X1) WAN** - IP address, network speed and devices connected to the WAN interface.
- **X2** - **X5** - user-defined interfaces.

SonicWALL PRO 5060

The SonicWALL PRO 5060 interfaces support up to 1 Gbps.

- **(X0) LAN** - IP address and network speed.
- **(X1) WAN** - IP address, network speed and devices connected to the WAN interface.
- **X2** - **X5** - user-defined interfaces.

SonicWALL TZ 170

- **LAN (LAN)** - IP address and network speed.
- **WAN (WAN)** - IP address, network speed and devices connected to the WAN interface.
- **OPT (Unassigned)** - user definable interface.

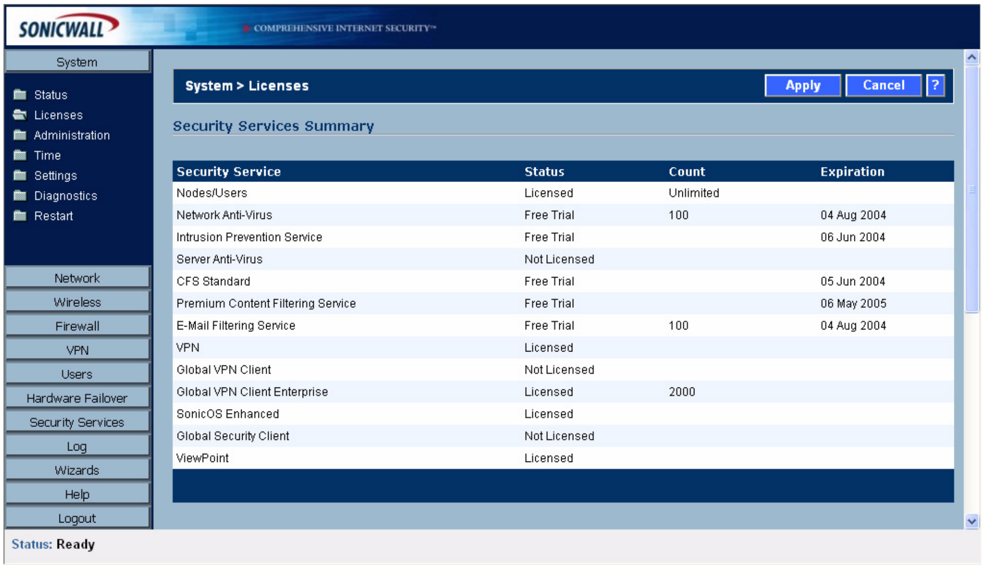
CHAPTER

4

Managing SonicWALL Security Services Licenses

System > Licenses

The **System>Licenses** page provides links to activate, upgrade, or renew SonicWALL Security Services licenses. From this page in the SonicWALL Management Interface, you can manage all the SonicWALL Security Services licensed for your SonicWALL security appliance. The information listed in the **Security Services Summary** table is updated from your mySonicWALL.com account. This chapter describes managing SonicWALL Security Services licenses from your mySonicWALL.com account directly from the SonicWALL Management Interface. The **System>Licenses** page also includes links to FREE trials of SonicWALL Security Services.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Licenses
Apply
Cancel
?

Security Services Summary

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
Network Anti-Virus	Free Trial	100	04 Aug 2004
Intrusion Prevention Service	Free Trial		06 Jun 2004
Server Anti-Virus	Not Licensed		
CFS Standard	Free Trial		05 Jun 2004
Premium Content Filtering Service	Free Trial		06 May 2005
E-Mail Filtering Service	Free Trial	100	04 Aug 2004
VPN	Licensed		
Global VPN Client	Not Licensed		
Global VPN Client Enterprise	Licensed	2000	
SonicOS Enhanced	Licensed		
Global Security Client	Not Licensed		
ViewPoint	Licensed		

Status: Ready

Security Services Summary

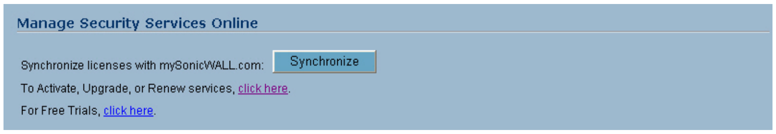
The **Security Services Summary** table lists the available and activated security services on the SonicWALL security appliance. The **Security Service** column lists all the available SonicWALL Security Services and upgrades available for the SonicWALL security appliance. The **Status** column indicates is the security service is activated (**Licensed**), available for activation (**Not Licensed**), or no longer active (**Expired**). The number of nodes/users allowed for the license is displayed in the **Count** column. The **Expiration** column displays the expiration date for any Licensed Security Service.

The information listed in the **Security Services Summary** table is updated from your mySonicWALL.com account the next time the SonicWALL security appliance automatically synchronizes with your mySonicWALL.com account (once a day) or you can click the link in **To synchronize licenses with mySonicWALL.com click here** in the **Manage Security Services Online** section.

➲ **Cross Reference:** *For more information on SonicWALL Security Services, see Part 9 Security Services.*

Manage Security Services Online

To activate, upgrade, or renew services, click the link in **To Activate, Upgrade, or Renew services, click here**. Click the link in **To synchronize licenses with mySonicWALL.com click here** to synchronize your mySonicWALL.com account with the **Security Services Summary** table.

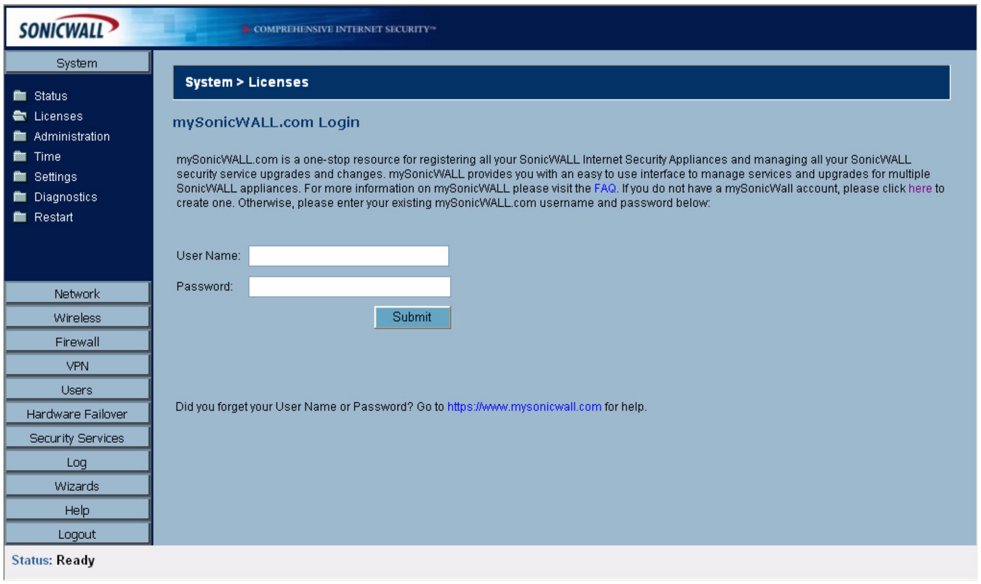

Manage Security Services Online
Synchronize

Synchronize licenses with mySonicWALL.com:

To Activate, Upgrade, or Renew services, click here.

For Free Trials, click here.

You can also get free trial subscriptions to SonicWALL Content Filter Service and Network Anti-Virus by clicking the **For Free Trials click here link**. When you click these links, the **mySonicWALL.com Login** page is displayed.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Licenses
mySonicWALL.com Login
Submit

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall account, please click here to create one. Otherwise, please enter your existing mySonicWALL.com username and password below:

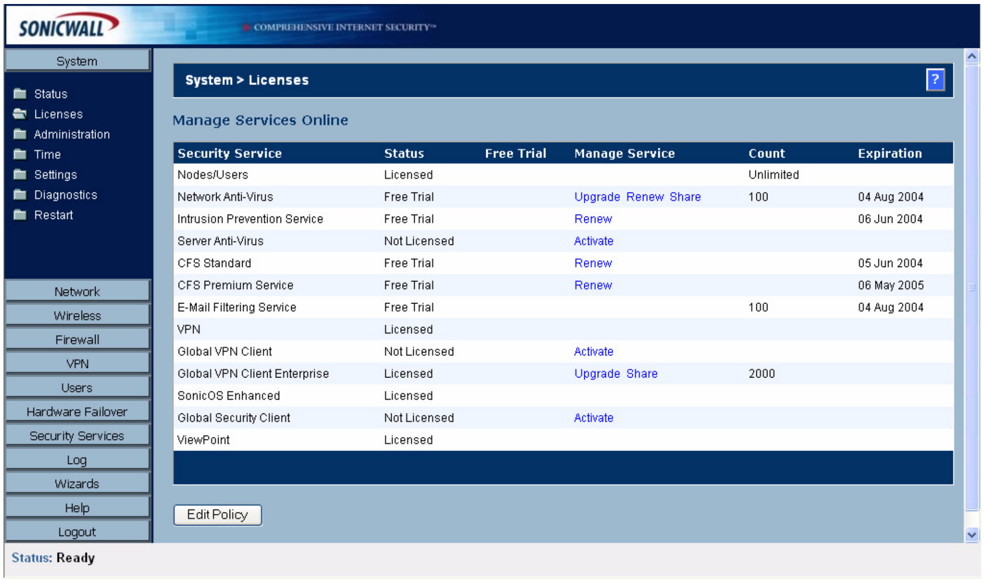
User Name:

Password:

Did you forget your User Name or Password? Go to https://www.mysonicwall.com for help.

Status: Ready

Enter your mySonicWALL.com account username and password in the **User Name** and Password fields and click Submit. The **Manage Services Online** page is displayed with licensing information from your mySonicWALL.com account.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Licenses
?
Edit Policy

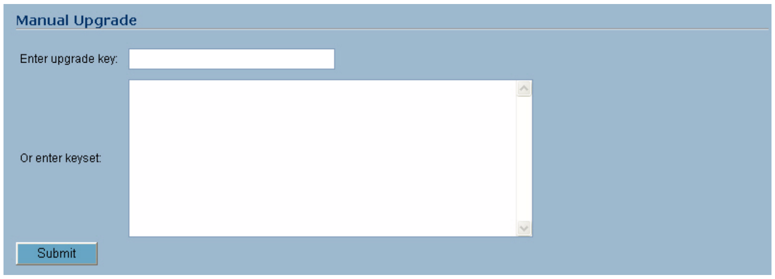
Manage Services Online

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Free Trial		Upgrade Renew Share	100	04 Aug 2004
Intrusion Prevention Service	Free Trial		Renew		06 Jun 2004
Server Anti-Virus	Not Licensed		Activate		
CFS Standard	Free Trial		Renew		05 Jun 2004
CFS Premium Service	Free Trial		Renew		06 May 2005
E-Mail Filtering Service	Free Trial			100	04 Aug 2004
VPN	Licensed				
Global VPN Client	Not Licensed		Activate		
Global VPN Client Enterprise	Licensed		Upgrade Share	2000	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Licensed				

Status: Ready

Manual Upgrade

Manual Upgrade allows you to activate your services by typing the service activation key supplied with the service subscription not activated on mySonicWALL.com. Type the activation key from the product into the **Enter upgrade key** field and click **Submit**.



Manual Upgrade

Enter upgrade key:

Or enter keyset:

Manual Upgrade for Closed Environments

If your SonicWALL security appliance is deployed in a high security environment that does not allow direct Internet connectivity from the SonicWALL security appliance, you can enter the encrypted license key information from http://www.mysonicwall.com manually on the **System>Licenses** page in the SonicWALL Management Interface.

Note: *Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your SonicWALL security appliance is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your SonicWALL security appliance.*

From a Computer Connected to the Internet

1. Make sure you have an account at http://www.mysonicwall.com and your SonicWALL security appliance is registered to the account before proceeding.

2. After logging into www.mysonicwall.com, click on your registered SonicWALL security appliance listed in **Registered SonicWALL Products**.

3. Click the **View License Keyset** link. The scrambled text displayed in the text box is the License Keyset for the selected SonicWALL security appliance and activated Security Services. Copy the Keyset text for pasting into the **System>Licenses** page or print the page if you plan to manually type in the Keyset into the SonicWALL security appliance.

From the Management Interface of your SonicWALL Security Appliance

4. Make sure your SonicWALL security appliance is running SonicOS Standard or Enhanced 2.1 (or higher).

5. Paste (or type) the Keyset (from the step 3) into the Keyset field in the **Manual Upgrade** section of the **System>Licenses** page (SonicOS).

6. Click the **Submit** or the **Apply** button to update your SonicWALL security appliance. The status field at the bottom of the page displays The configuration has been updated.

7. You can generate the **System>Diagnostics>Tech Support Report** to verify the upgrade details.

Note: *After the manual upgrade, the **System>Licenses** page does not contain any registration and upgrade information.*

Tip: *The warning message: **SonicWALL Registration Update Needed. Please update your registration information** remains on the **System>Status** page after you have registered your SonicWALL security appliance. Ignore this message.*

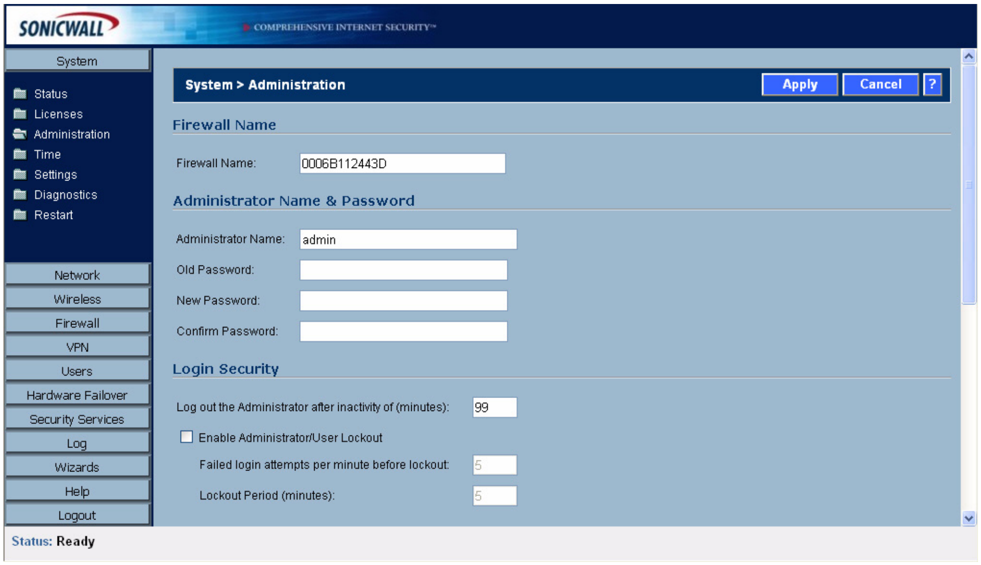
CHAPTER W

5

Configuring SonicWALL Security Appliance Administration Settings

System > Administration

The System Administration page provides settings for the configuration of SonicWALL security appliance for secure and remote management. You can manage the SonicWALL using a variety of methods, including HTTPS, SNMP or SonicWALL Global Management System (SonicWALL GMS).


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Administration
Apply
Cancel
?

Firewall Name

Firewall Name: 0006B112443D

Administrator Name & Password

Administrator Name: admin
Old Password:
New Password:
Confirm Password:

Login Security

Log out the Administrator after inactivity of (minutes): 99
☐ Enable Administrator/User Lockout
Failed login attempts per minute before lockout: 5
Lockout Period (minutes): 5

Status: Ready

Firewall Name

The **Firewall Name** uniquely identifies the SonicWALL security appliance and defaults to the serial number of the SonicWALL. The serial number is also the MAC address of the unit. To change the **Firewall Name**, type a unique alphanumeric name in the **Firewall Name** field. It must be at least 8 characters in length.

Administrator Name & Password

The **Administrator Name** can be changed from the default setting of **admin** to any word using alphanumeric characters up to 32 characters in length. To create an new administrator name, type the new name in the **Administrator Name** field. Click **Apply** for the changes to take effect on the SonicWALL.

Changing the Administrator Password

To set a new password for SonicWALL Management Interface access, type the old password in the **Old Password** field, and the new password in the **New Password** field. Type the new password again in the **Confirm New Password** field and click **Apply**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

✓ **Tip:** *It's recommended you change the default password* ***password*** *to your own custom password.*

Login Security

The **Log out the Administrator Inactivity Timeout after inactivity of (minutes)** setting allows you to set the length of inactivity time that elapses before you are automatically logged out of the Management Interface. By default, the SonicWALL security appliance logs out the administrator after 5 minutes of inactivity. The inactivity timeout can range from 1 to 99 minutes. Click **Apply**, and a message confirming the update is displayed at the bottom of the browser window.

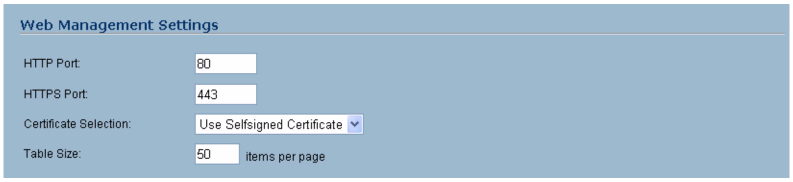
✓ **Tip:** *If the Administrator Inactivity Timeout is extended beyond 5 minutes, you should end every management session by clicking Logout to prevent unauthorized access to the SonicWALL security appliance's Management Interface.*

Enable Administrator/User Lockout

You can configure the SonicWALL security appliance to lockout an administrator or a user if the login credentials are incorrect. Select the **Enable Administrator/User Lockout on login failure** checkbox to prevent users from attempting to log into the SonicWALL security appliance without proper authentication credentials. Type the number of failed attempts before the user is locked out in the **Failed login attempts per minute before lockout** field. Type the length of time that must elapse before the user attempts to log into the SonicWALL again in the **Lockout Period (minutes)** field.

▲ **Alert:** *If the administrator and a user are logging into the SonicWALL using the same source IP address, the administrator is also locked out of the SonicWALL. The lockout is based on the source IP address of the user or administrator.*

Web Management Settings



Web Management Settings

HTTP Port: 80

HTTPS Port: 443

Certificate Selection: Use Selfsigned Certificate

Table Size: 50 items per page

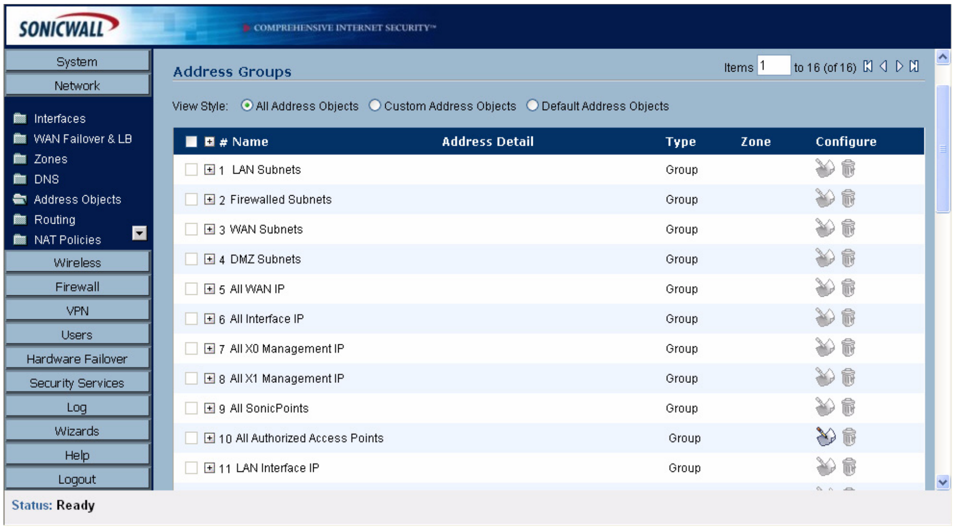
The SonicWALL security appliance can be managed using HTTP or HTTPS and a Web browser. Both HTTP and HTTPS are enabled by default. The default port for HTTP is port 80, but you can configure access through another port. Type the number of the desired port in the **Port** field, and click **Apply**. However, if you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWALL security applaince. For example, if you configure the port to be 76, then you must type <LAN IP Address>:76 into the Web browser, i.e. <http://192.168.168.1:76>. The default port for HTTPS management is **443**.

You can add another layer of security for logging into the SonicWALL security appliance by changing the default port. To configure another port for HTTPS management, type the preferred port number into the **Port** field, and click **Update**. For example, if you configure the HTTPS Management Port to be 700, then you must log into the SonicWALL using the port number as well as the IP address, for example, <https://192.168.168.1:700> to access the SonicWALL.

The **Certificate Selection** menu allows you to use a self-signed certificate (**Use Self-signed Certificate**), which allows you to continue using a certificate without downloading a new one each time you log into the SonicWALL security appliance. You can also choose **Import Certificate** to select an imported certificate from the **VPN>Local Certificates** page to use for authentication to the Management Interface.

Changing the Default Size for SonicWALL Management Interface Tables

The SonicWALL Management Interface allows you to control the display of large tables of information across all tables in the management Interface; for example the table on the **Network>Address Objects** page.



Address Groups

Items 1 to 16 (of 16)

View Style: ● All Address Objects ○ Custom Address Objects ○ Default Address Objects

# Name	Address Detail	Type	Zone	Configure
☐ ⊞ 1 LAN Subnets		Group		
☐ ⊞ 2 Firewalled Subnets		Group		
☐ ⊞ 3 WAN Subnets		Group		
☐ ⊞ 4 DMZ Subnets		Group		
☐ ⊞ 5 All WAN IP		Group		
☐ ⊞ 6 All Interface IP		Group		
☐ ⊞ 7 All X0 Management IP		Group		
☐ ⊞ 8 All X1 Management IP		Group		
☐ ⊞ 9 All SonicPoints		Group		
☐ ⊞ 10 All Authorized Access Points		Group		
☐ ⊞ 11 LAN Interface IP		Group		

Status: Ready

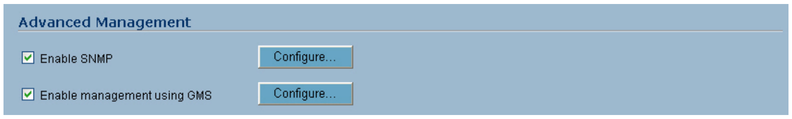
You can change the default table page size in all tables displayed in the SonicWALL Management Interface from the default 50 items per page to any size ranging from 1 to 5,000 items.

To change the default table size:

1. Enter the maximum table size number in the **Table Size** field.
2. Click **Apply**.

Advanced Management

You can manage the SonicWALL security appliance using SNMP or SonicWALL Global Management System. The following sections explain how to configure the SonicWALL for management by these two options.



Advanced Management

☑ Enable SNMP

☑ Enable management using GMS

➲ **Cross Reference:** *For more information on SonicWALL Global Management System, go to http://www.sonicwall.com.*

Enabling SNMP Management

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the SonicWALL security appliance and receive notification of critical events as they occur on the network. The SonicWALL security appliance supports SNMP v1/v2c and all relevant Management Information Base II (MIB) groups except **egp** and **at**. The SonicWALL security appliance replies to SNMP Get commands for MIBII via any interface and supports a custom SonicWALL MIB for generating trap messages. The custom SonicWALL MIB is available for download from the SonicWALL Web site and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC.

Configuring SNMP Management

To enable SNMP on the SonicWALL security appliance, log into the Management interface and click **System**, then Administration. Select the **Enable SNMP** checkbox, and then click **Configure**.

1. Type the host name of the SonicWALL security appliance in the **System Name** field.
2. Type the network administrator's name in the **System Contact** field.
3. Type an e-mail address, telephone number, or pager number in the **System Location** field.
4. Type a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field.
5. Type a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.
6. Type the IP address or host name of the SNMP management system receiving SNMP traps in the Host 1 through Host 4 fields. You must configure at least one IP address or host name, but up to four addresses or host names can be used.
7. Click **OK**.

Configuring Log/Log Settings for SNMP

Trap messages are generated only for the alert message categories normally sent by the SonicWALL security appliance. For example, attacks, system errors, or blocked Web sites generate trap messages. If none of the categories are selected on the **Log>Settings** page, then no trap messages are generated.

Configuring SNMP as a Service and Adding Rules

By default, the SonicWALL security appliance responds only to **Get SNMP** messages received on its LAN interface. Appropriate rules must be configured to allow SNMP traffic to and from the WAN interface. SNMP trap messages can be sent via the LAN or WAN.

➲ **Cross Reference:** *For instructions on adding services and rules to the SonicWALL security appliance, see Part 5 Firewall.*

If your SNMP management system supports discovery, the SonicWALL security appliance agent automatically discover the SonicWALL security appliance on the network. Otherwise, you must add the SonicWALL security appliance to the list of SNMP-managed devices on the SNMP management system.

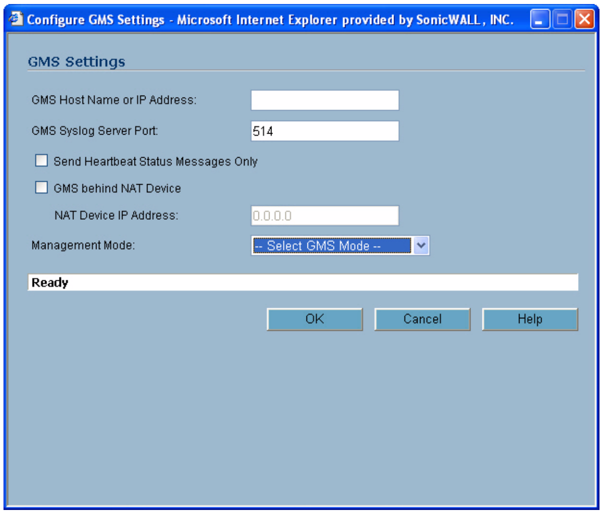
Enable GMS Management

You can configure the SonicWALL security appliance to be managed by SonicWALL Global Management System (SonicWALL GMS).

Configuring the SonicWALL Security Appliance for GMS Management

To configure the SonicWALL security appliance for GMS management:

1. Select the **Enable Management using GMS** checkbox, then click **Configure**. The **Configure GMS Settings** window is displayed.



Configure GMS Settings - Microsoft Internet Explorer provided by SonicWALL, INC.

GMS Settings

GMS Host Name or IP Address:

GMS Syslog Server Port: 514

☐ Send Heartbeat Status Messages Only

☐ GMS behind NAT Device

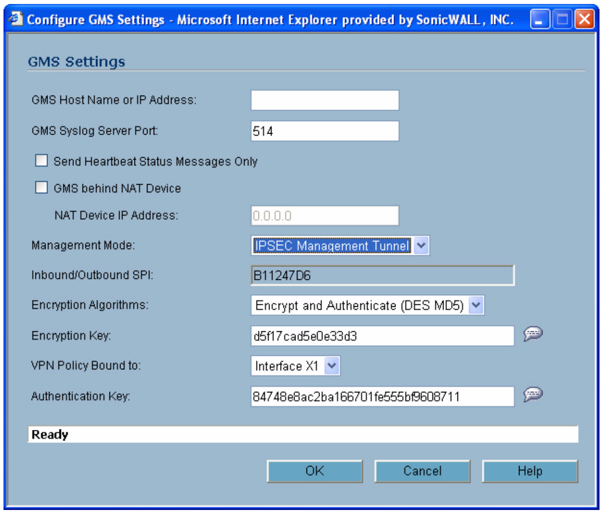
NAT Device IP Address: 0.0.0.0

Management Mode: -- Select GMS Mode --

Ready

2. Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.
3. Enter the port in the **GMS Syslog Server Port** field. The default value is **514**.
4. Select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages.
5. Select **GMS behind NAT Device** if the GMS Console is placed behind a device using NAT on the network. Type the IP address of the NAT device in the **NAT Device IP Address** field.
6. Select one of the following GMS modes from the Management Mode menu.

   IPSEC Management Tunnel - Selecting this option allows the SonicWALL security appliance to be managed over an IPSec VPN tunnel to the GMS management console. The default IPSec VPN settings are displayed. Select **GMS behind NAT Device** if applicable to the GMS installation, and enter the IP address in the **NAT Device IP Address** field. The default VPN policy settings are displayed at the bottom of the **Configure GMS Settings** window.



Configure GMS Settings - Microsoft Internet Explorer provided by SonicWALL, INC.

GMS Settings

GMS Host Name or IP Address:

GMS Syslog Server Port: 514

☐ Send Heartbeat Status Messages Only

☐ GMS behind NAT Device

NAT Device IP Address: 0.0.0.0

Management Mode: IPSEC Management Tunnel

Inbound/Outbound SPI: B11247D6

Encryption Algorithms: Encrypt and Authenticate (DES MD5)

Encryption Key: d5f17cad5e0e33d3

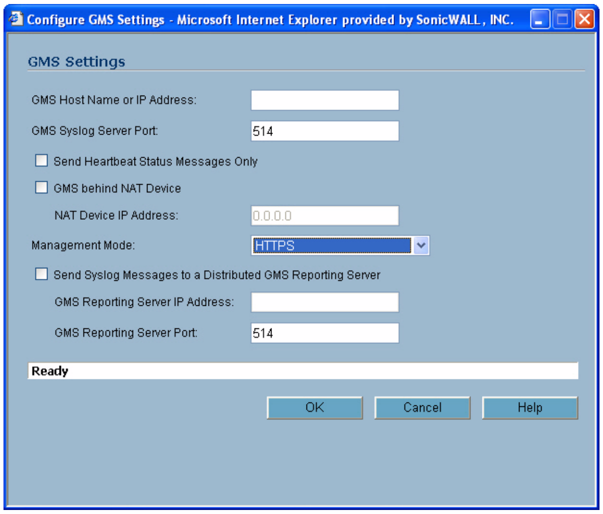
VPN Policy Bound to: Interface X1

Authentication Key: 84748e8ac2ba166701fe555bf9608711

Ready

Existing Tunnel - If this option is selected, the GMS server and the SonicWALL security appliance already have an existing VPN tunnel over the connection. Enter the GMS host name or IP address in the **GMS Host Name or IP Address** field. Enter the port number in the **Syslog Server Port** field.

HTTPS - If this option is selected, HTTPS management is allowed from two IP addresses: the GMS Primary Agent and the Standby Agent IP address. The SonicWALL security appliance also sends encrypted syslog packets and SNMP traps using 3DES and the SonicWALL security appliance administrator’s password. The following configuration settings for HTTPS management mode are displayed:



Configure GMS Settings - Microsoft Internet Explorer provided by SonicWALL, INC.

GMS Settings

GMS Host Name or IP Address:

GMS Syslog Server Port: 514

☐ Send Heartbeat Status Messages Only

☐ GMS behind NAT Device

NAT Device IP Address: 0.0.0.0

Management Mode: HTTPS

☐ Send Syslog Messages to a Distributed GMS Reporting Server

GMS Reporting Server IP Address:

GMS Reporting Server Port: 514

Ready

Send Syslog Messages in Cleartext Format - Sends heartbeat messages as cleartext.

Send Syslog Messages to a Distributed GMS Reporting Server - Sends regular heartbeat messages to both the GMS Primary and Standby Agent IP address. The regular heartbeat messages are sent to the specified GMS reporting server and the reporting server port.

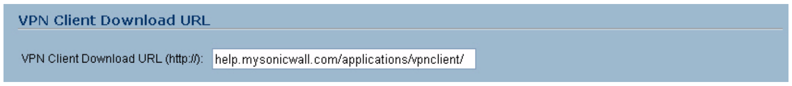
GMS Reporting Server IP Address - Enter the IP address of the GMS Reporting Server, if the server is separate from the GMS management server.

GMS Reporting Server Port - Enter the port for the GMS Reporting Server. The default value is 514

7 Click **OK**.

VPN Client Download URL

The **VPN Client Download URL** provides a field for entering the URL address of a site for downloading the SonicWALL Global VPN Client application, when a user is prompted to use the Global VPN Client for access to the network.



VPN Client Download URL

VPN Client Download URL (http://): help.mysonicwall.com/applications/vpnclient/

The default URL http://help.mysonicwall.com/applications/vpnclient displays the SonicWALL Global VPN Client download site. You can point to any URL where you provide the SonicWALL Global VPN Client application.

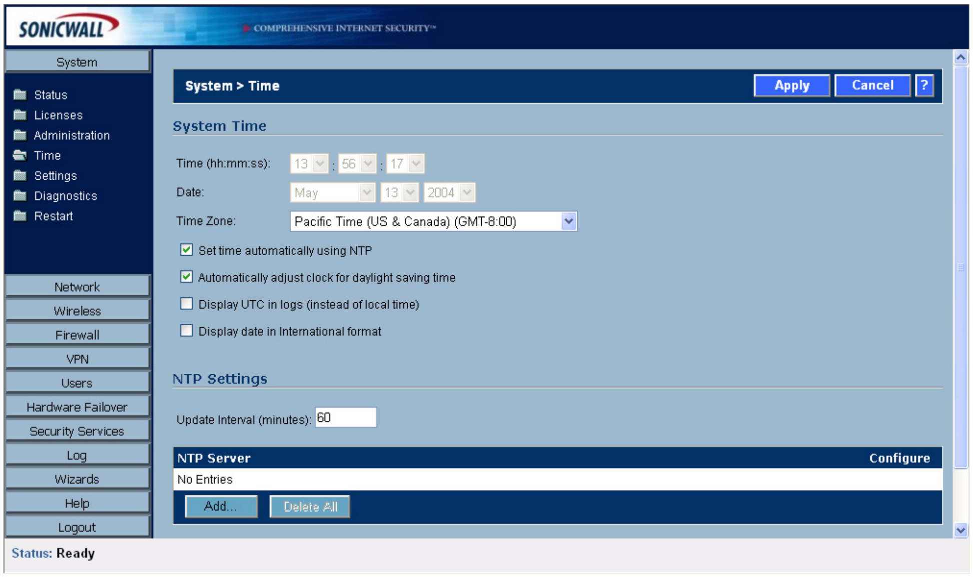
CHAPTER

6

Configuring Time Settings

System > Time

The **System>Time** page defines the time and date settings to time stamp log events, to automatically update SonicWALL Security Services, and for other internal purposes. iBy default, the SonicWALL security appliance uses an internal list of public NTP servers to automatically update the time. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Time
Apply
Cancel
?
Add...
Delete All

System Time

Time (hh:mm:ss): 13 : 56 : 17

Date: May 13 2004

Time Zone: Pacific Time (US & Canada) (GMT-8:00)

☑ Set time automatically using NTP

☑ Automatically adjust clock for daylight saving time

☐ Display UTC in logs (instead of local time)

☐ Display date in International format

NTP Settings

Update Interval (minutes): 60

NTP Server	Configure
No Entries	

Status: Ready

System Time

To select your time zone and automatically update the time, choose the time zone from the **Time Zone** menu. The **Use NTP to set time automatically** is activated by default to use the NTP (Network Time Protocol) to set time automatically. If you want to set your time manually, uncheck this setting. Select the time in the 24-hour format using the **Time (hh:mm:ss)** menus and the date from the **Date** menus. **Automatically adjust clock for daylight saving changes** is activated by default to enable automatic adjustments for daylight savings time.

Selecting **Display UTC in logs (instead of local time)** specifies the use universal time (UTC) rather than local time for log events.

Selecting **Display time in International format** displays the date in International format, with the day preceding the month.

After selecting your System Time settings, click **Apply**.

NTP Settings

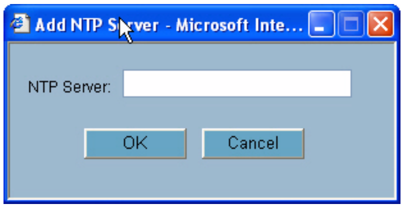
Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond.

✓ **Tip:** *The SonicWALL security appliance uses an internal list of NTP servers so manually entering a NTP server is optional.*

Select **Use NTP to set time automatically** if you want to use your local server to set the SonicWALL security appliance clock. You can also configure **Update Interval (minutes)** for the NTP server to update the SonicWALL security appliance. The default value is 60 minutes.

To add an NTP server to the SonicWALL security appliance configuration

1. Click **Add**. The **Add NTP Server** window is displayed.



2. Type the IP address of an NTP server in the **NTP Server** field.
3. Click **OK**.
4. Click **Apply** on the **System>Time** page to update the SonicWALL security appliance.

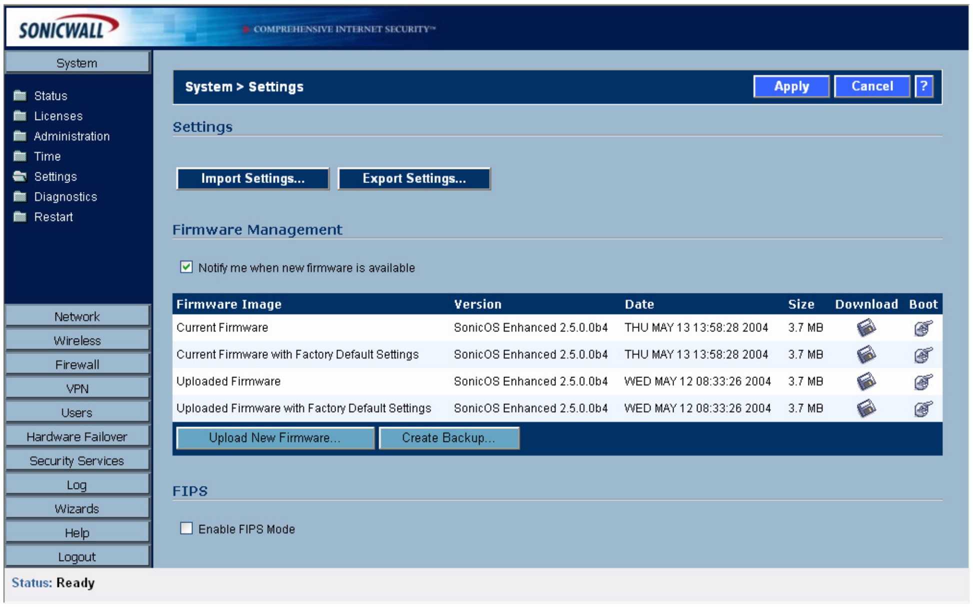
To delete an NTP server, highlight the IP address and click **Delete**. Or, click **Delete All** to delete all servers.

CHAPTER 7

Managing SonicWALL Security Appliance Firmware

System > Settings

This **System>Settings** page allows you to manage your SonicWALL security appliance's SonicOS versions and preferences.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Settings
Apply
Cancel
?
Settings
Import Settings...
Export Settings...
Firmware Management
Upload New Firmware...
Create Backup...
FIPS

☑ Notify me when new firmware is available

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 2.5.0.0b4	THU MAY 13 13:58:28 2004	3.7 MB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 2.5.0.0b4	THU MAY 13 13:58:28 2004	3.7 MB		
Uploaded Firmware	SonicOS Enhanced 2.5.0.0b4	WED MAY 12 08:33:26 2004	3.7 MB		
Uploaded Firmware with Factory Default Settings	SonicOS Enhanced 2.5.0.0b4	WED MAY 12 08:33:26 2004	3.7 MB		

☐ Enable FIPS Mode

Status: Ready

Settings

Import Settings

To import a previously saved preferences file into the SonicWALL security appliance, follow these instructions:

1. Click **Import Settings** to import a previously exported preferences file into the SonicWALL security appliance. The **Import Settings** window is displayed.
2. Click **Browse** to locate the file which has a *.exp file name extension.

3 Select the preferences file.
4 Click **Import**, and restart the firewall.

Export Settings

To export configuration settings from the SonicWALL security appliance, use the instructions below:

1 Click **Export Settings**.
2 Click **Export**.
3 Click **Save**, and then select a location to save the file. The file is named “sonicwall.exp” but can be renamed.
4 Click **Save**. This process can take up to a minute. The exported preferences file can be imported into the SonicWALL security appliance if it is necessary to reset the firmware.

Firmware Management

The **Firmware Management** section provides settings that allow for easy firmware upgrade and preferences management. The **Firmware Management** section allows you to:

- Upload and download firmware images and system settings.
- Boot to your choice of firmware and system settings.
- Manage system backups.
- Easily return your SonicWALL security appliance to the previous system state.

Note: *SonicWALL security appliance **SafeMode**, which uses the same settings used **Firmware Management**, provides quick recovery from uncertain configuration states.*

Automatic Notification of New Firmware

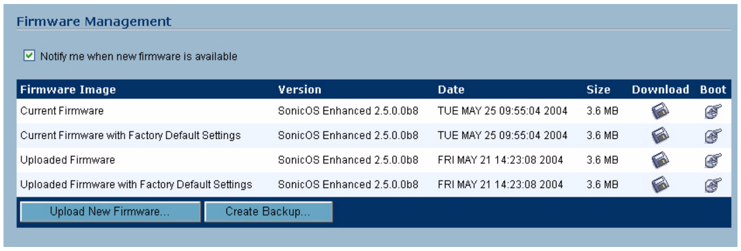
To receive automatic notification of new firmware, select the **Notify me when new firmware is available** check box. If you enable this feature, the SonicWALL security appliance sends a status message to the SonicWALL firmware server daily with the following information:

- **SonicWALL Serial Number**
- **Product Type**
- **Current Firmware Version**
- **Language**
- **Currently Available Memory**
- **ROM Version**

Alert: *After the initial 90 days from purchase, firmware updates are available only to registered users with a valid support contract. You must register your SonicWALL at <https://www.mysonicwall.com>.*

If a new firmware version becomes available, the message **New SonicWALL Firmware Version is available**. Click here for details on this latest release appears in System Messages on the **System>Status** page. Clicking the here link displays the Release Notes for the new firmware.

Firmware Management Table



Firmware Management

☑ Notify me when new firmware is available

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 2.5.0.0b8	TUE MAY 25 09:55:04 2004	3.6 MB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 2.5.0.0b8	TUE MAY 25 09:55:04 2004	3.6 MB		
Uploaded Firmware	SonicOS Enhanced 2.5.0.0b8	FRI MAY 21 14:23:08 2004	3.6 MB		
Uploaded Firmware with Factory Default Settings	SonicOS Enhanced 2.5.0.0b8	FRI MAY 21 14:23:08 2004	3.6 MB		

The Firmware Management table displays the following information:

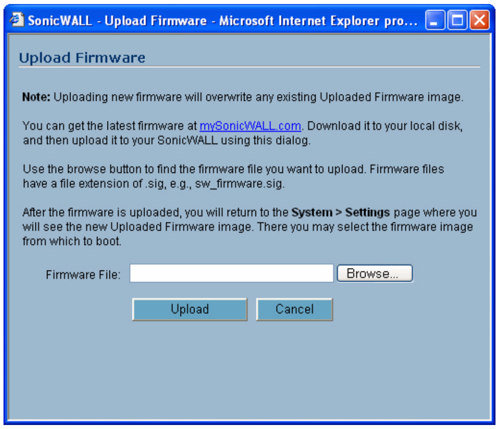
- **Firmware Image** - In this column, four types of firmware images are listed:
    - **Current Firmware** - firmware currently loaded on the SonicWALL security appliance.
    - **Current Firmware with Factory Default Settings** - rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, username, and password.
    - **Uploaded Firmware** - the latest uploaded version from mySonicWALL.com.
    - **Uploaded Firmware with Factory Default Settings** - the latest version uploaded with factory default settings.
    - **System Backup** - a firmware image created by clicking **Create Backup**.
- **Version** - the firmware version.
- **Date** - the day, date, and time of downloading the firmware.
- **Size** - the size of the firmware file in Megabytes (MB).
- **Download** - clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - clicking the icon reboots the SonicWALL security appliance with the firmware version listed in the same row.

Alert: *Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the **Current Firmware** image. On the TZ 170, the uploaded firmware images are removed from the table after rebooting the SonicWALL security appliance.*

Alert: *When uploading firmware to the SonicWALL security appliance, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.*

Updating Firmware Manually

Click **Upload New Firmware** to upload new firmware to the SonicWALL security appliance. The **Upload Firmware** window is displayed. Browse to the firmware file located on your local drive. Click **Upload** to upload the new firmware to the SonicWALL security appliance.


SonicWALL - Upload Firmware - Microsoft Internet Explorer pro...
Upload Firmware
Firmware File:
Browse...
Upload
Cancel

Note: Uploading new firmware will overwrite any existing Uploaded Firmware image.

You can get the latest firmware at mySonicWALL.com. Download it to your local disk, and then upload it to your SonicWALL using this dialog.

Use the browse button to find the firmware file you want to upload. Firmware files have a file extension of .sig, e.g., sw_firmware.sig.

After the firmware is uploaded, you will return to the **System > Settings** page where you will see the new Uploaded Firmware image. There you may select the firmware image from which to boot.

Creating a Backup Firmware Image

When you click **Create Backup**, the SonicWALL security appliance takes a “snapshot” of your current system state, firmware and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing **System Backup** firmware image as necessary.

SafeMode - Rebooting the SonicWALL Security Appliance

SafeMode allows easy firmware and preferences management as well as quick recovery from uncertain configuration states. It is no longer necessary to reset the firmware by pressing and holding the Reset button on the appliance. Pressing the Reset button for one second launches the SonicWALL security appliance into SafeMode. SafeMode allows you to select the firmware version to load and reboot the SonicWALL security appliance.

Note: *Because there are hardware differences between the TZ 170 and the PRO 2040/PRO 3060/PRO 4060/PRO 5060, Safe Mode on the TZ 170 cannot store as many firmware images as the PRO 2040/3060. After rebooting, the TZ 170 does not retain uploaded firmware images.*

To access the SonicWALL security appliance using SafeMode, press the Reset button for 1 second. After the SonicWALL security appliance reboots, open your Web browser and enter the current IP address of the SonicWALL security appliance or the default IP address: *192.168.168.168*. The SafeMode page is displayed:

SafeMode allows you to do any of the following:

- Upload and download firmware images to the SonicWALL security appliance.
- Upload and download system settings to the SonicWALL security appliance.
- Boot to your choice of firmware options.
- Create a system backup file.
- Return your SonicWALL security appliance to a previous system state.

System Information

System Information for the SonicWALL security appliance is retained and displayed in this section.

Firmware Management

The **Firmware Management** table has the following columns:

- **Firmware Image** - In this column, five types of firmware images are listed:

  - Current Firmware, firmware currently loaded on the SonicWALL security appliance

  - **Current Firmware with Factory Default Settings**, rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password

  - **Uploaded Firmware**, the last version uploaded from mysonicwall.com

  - **Uploaded Firmware with Factory Default Settings,** rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password

  - **System Backup**, a firmware image created by clicking **Create Backup**.
- **Version** - The firmware version is listed in this column.
- **Date** - The day, date, and time of downloading the firmware.
- **Size** - The size of the firmware file in Megabytes (MB).
- **Download** - Clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - Clicking the icon reboots the SonicWALL security appliance with the firmware version listed in the same row.

Note: *Clicking* ***Boot*** *next to any firmware image overwrites the existing current firmware image making it the Current Firmware image.*

Click **Boot** in the firmware row of your choice to restart the SonicWALL security appliance.

FIPS (PRO 3060/PRO 4060/PRO 5060)

When operating in FIPS (Federal Information Processing Standard) Mode, the SonicWALL security appliance supports FIPS-Compliant security. Among the FIPS-compliant features of the SonicWALL security appliance include PRNG based on SHA-1 and only FIPS-approved algorithms are supported (DES, 3DES, and AES with SHA-1).

Select **Enable FIPS Mode** to enable the SonicWALL security appliance to comply with FIPS. When you check this setting, a dialog box is displayed with the following message: **Warning! Modifying the FIPS mode will disconnect all users and restart the device. Click OK to proceed**. Click Clicking Boot next to any firmware image overwrites the existing current firmware image making it the Current Firmware image. The SonicWALL security appliance reboots in FIPS Mode.

To return to normal operation, uncheck the **Enable FIPS Mode** check box. The SonicWALL security appliance reboots into non-FIPS mode.

Alert: *When using the SonicWALL security appliance for FIPS-compliant operation, the tamper-evident sticker that is affixed to the SonicWALL security appliance must remain in place and untouched.*

CHAPTER

8

Using Diagnostic Tools & Restarting the SonicWALL Security Appliance

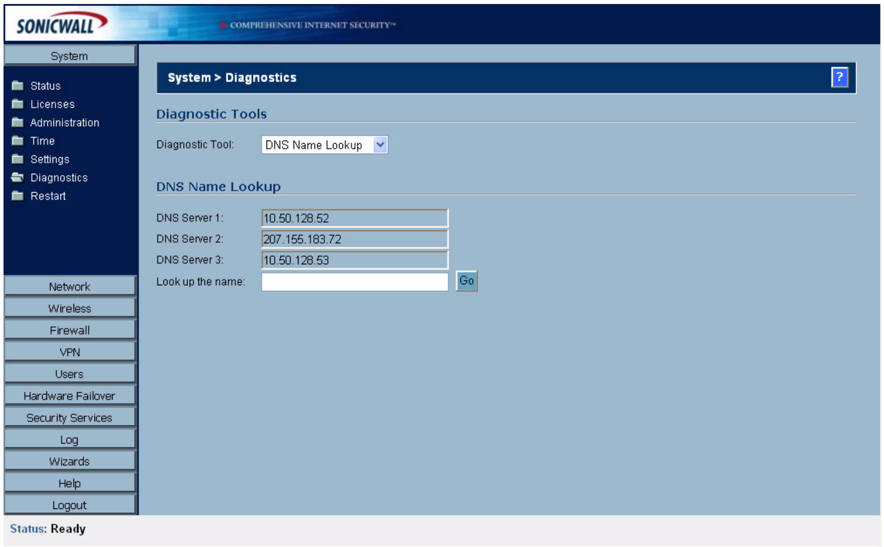
System > Diagnostics

The **System>Diagnostics** page provides a a collection of diagnostic tools to help troubleshoot network problems:

- DNS Name Lookup
- Find Network Path
- Ping
- Packet Trace
- Tech Support Report
- Trace Route

Diagnostic Tools

You can choose any of the following diagnostic tools from the **Diagnostic Tool** menu.



System > Diagnostics

Diagnostic Tools

Diagnostic Tool: DNS Name Lookup

DNS Name Lookup

DNS Server 1: 10.50.128.52
DNS Server 2: 207.155.183.72
DNS Server 3: 10.50.128.53
Look up the name:

Status: Ready

DNS Name Lookup

The SonicWALL security appliance has a DNS lookup tool that returns the IP address of a domain name. Or, if you type an IP address, it returns the domain name for that address.

1. Type the host name or IP address in the **Look up name** field. Do not add http to the host name.
2. The SonicWALL security appliance queries the DNS Server and displays the result in the **Result** section. It also displays the IP address of the DNS Server used to perform the query.

The **DNS Name Lookup** section also displays the IP addresses of the DNS Servers configured on the SonicWALL security appliance. If there is no IP address or IP addresses in the **DNS Server** fields, you must configure them on the **Network>Settings** page.

Find Network Path

Find Network Path indicates if an IP host is located on the WAN, DMZ, LAN, or other zone. This can diagnose a network configuration problem on the SonicWALL security appliance. For example, if the SonicWALL security appliance indicates that a computer on the Internet is located on the LAN, then the network or Intranet settings may be misconfigured. **Find Network Path** can be used to determine if a target device is located behind a network router and the Ethernet address of the target device. It also displays the gateway the device is using and helps isolate configuration problems.

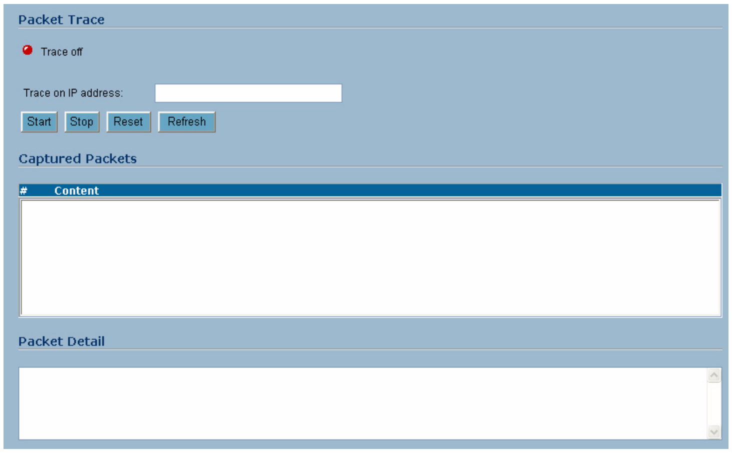
Ping

The **Ping** test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the SonicWALL security appliance is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

1. Select **Ping** from the **Diagnostic Tool** menu.
2. Type the IP address or host name of the target device and click **Go**.
3. If the test is successful, the SonicWALL security appliance returns a message saying the IP address is alive and the time to return in milliseconds (ms).

Packet Trace

The **Packet Trace** tool tracks the status of a communications stream as it moves from source to destination. This is a useful tool to determine if a communications stream is being stopped at the SonicWALL security appliance, or is lost on the Internet.



To interpret this tool, it is necessary to understand the three-way handshake that occurs for every TCP connection. The following displays a typical three-way handshake initiated by a host on the SonicWALL security appliance LAN to a remote host on the WAN.

- TCP received on LAN [SYN]

  From 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)

  To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

The SonicWALL security appliance receives SYN from LAN client.

- TCP sent on WAN [SYN]

  From 207.88.211.116 / 1937 (00:40:10:0c:01:4e)

  To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

The SonicWALL security appliance forwards SYN from LAN client to remote host.

- TCP received on WAN [SYN,ACK]

  From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

  To 207.88.211.116 / 1937 (00:40:10:0c:01:4e)

The SonicWALL security appliance receives SYN,ACK from remote host.

- TCP sent on LAN [SYN,ACK]

  From 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

  To 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)

The SonicWALL security appliance forwards SYN,ACK to LAN client.

- TCP received on LAN [ACK]

  From 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)

  To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

Client sends a final ACK, and waits for start of data transfer.

- TCP sent on WAN [ACK]

  From 207.88.211.116 / 1937 (00:40:10:0c:01:4e

To 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

The SonicWALL security appliance forwards the client ACK to the remote host and waits for the data transfer to begin.

When using packet traces to isolate network connectivity problems, look for the location where the three-way handshake is breaking down. This helps to determine if the problem resides with the SonicWALL security appliance configuration, or if there is a problem on the Internet.

Select **Packet Trace** from the **Diagnostic tool** menu.

Tip: *Packet Trace requires an IP address. The SonicWALL security appliance DNS Name Lookup tool can be used to find the IP address of a host.*

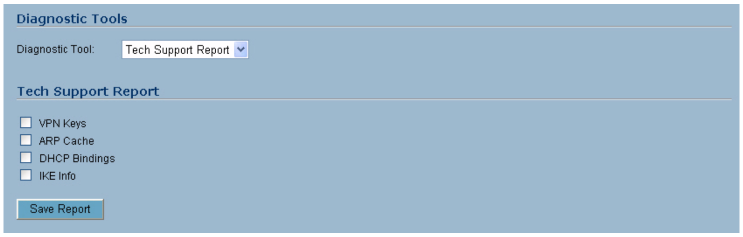
1. Type the IP address of the remote host in the **Trace on IP address** field, and click **Start**. You must type an IP address in the **Trace on IP address** field; do not type a host name, such as “www.yahoo.com”. The **Trace is off** turns from red to green with Trace Active displayed.
2. Contact the remote host using an IP application such as Web, FTP, or Telnet.
3. Click **Refresh** and the packet trace information is displayed.
4. Click **Stop** to terminate the packet trace, and **Reset** to clear the results.

The **Captured Packets** table displays the packet number and the content of the packet, for instance, *ARP Request send on WAN 42 bytes*.

Select a packet in the **Captured Packets** table to display packet details. Packet details include the packet number, time, content, source of the IP address, and the IP address destination.

Tech Support Report

The **Tech Support Report** generates a detailed report of the SonicWALL security appliance configuration and status, and saves it to the local hard disk. This file can then be e-mailed to SonicWALL Technical Support to help assist with a problem.


Diagnostic Tool: Tech Support Report

Alert: *You must register your SonicWALL security appliance on mySonicWALL.com to receive technical support.*

Before e-mailing the Tech Support Report to the SonicWALL Technical Support team, complete a Tech Support Request Form at <https://www.mysonicwall.com>. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows SonicWALL Technical Support to provide you with better service.

In the **Tools** section, select **Tech Support Report** from the **Select a diagnostic tool** menu. Four **Report Options** are available in the **Tech Support Report** section:

- **VPN Keys** - saves shared secrets, encryption, and authentication keys to the report.
- **ARP Cache** - saves a table relating IP addresses to the corresponding MAC or physical addresses.
- **DHCP Bindings** - saves entries from the SonicWALL DHCP server.
- **IKE Info** - saves current information about active IKE configurations.

Generating a Tech Support Report

1. Select **Tech Support Report** from the **Choose a diagnostic tool** menu.
2. Select the **Report Options** to be included with your e-mail.
3. Click **Save Report** to save the file to your system. When you click **Save Report**, a warning message is displayed.
4. Click **OK** to save the file. Attach the report to your **Tech Support Request** e-mail.

Trace Route

Trace Route is a diagnostic utility to assist in diagnosing and troubleshooting router connections on the Internet. By using Internet Connect Message Protocol (ICMP) echo packets similar to Ping packets, **Trace Route** can test interconnectivity with routers and other hosts that are farther and farther along the network path until the connection fails or until the remote host responds.

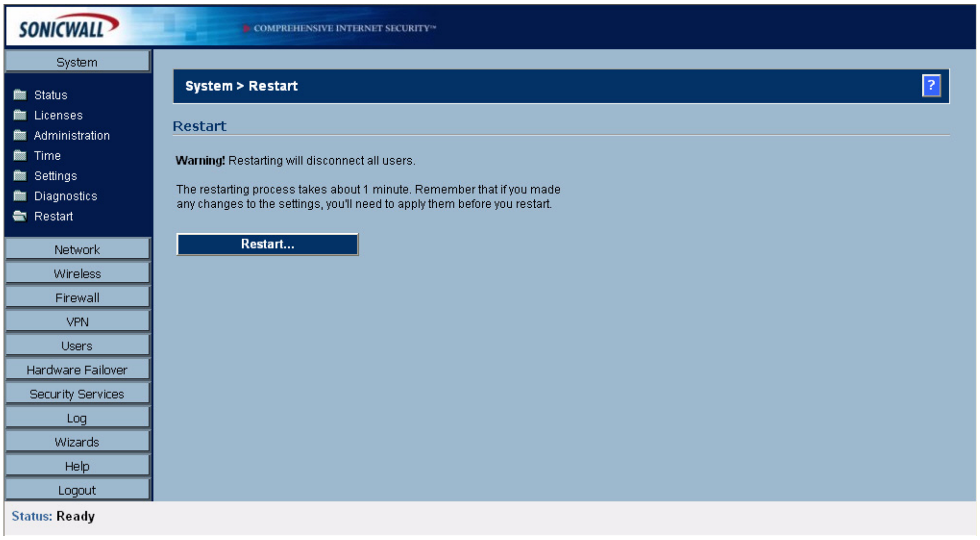
Type the IP address or domain name of the destination host. For example, type yahoo.com and click **Go**.

A second window is displayed with each hop to the destination host.

By following the route, you can diagnose where the connection fails between the SonicWALL security appliance and the destination.

System > Restart

Click **Restart** to display the **System>Restart** page. The SonicWALL security appliance can be restarted from the Web Management interface. Click **Restart SonicWALL** and then click **Yes** to confirm the restart. The SonicWALL security appliance takes approximately one minute to restart, and the yellow Test light is lit during the restart.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Restart
?
Restart
Restart...

Warning! Restarting will disconnect all users.

The restarting process takes about 1 minute. Remember that if you made any changes to the settings, you'll need to apply them before you restart.

Status: Ready

✓ **Tip:** *If you made any configuration changes to the SonicWALL security appliance, make sure your apply them before restarting the SonicWALL security appliance or the changes will not be saved.*

▲ **Alert:** *Restarting the SonicWALL security appliance will disconnect all users.*

PART

3

Network

:

CHAPTER W
9
Configuring Interfaces

Network > Interfaces

The **Network>Interfaces** page includes interface objects that are directly linked to physical interfaces. The SonicOS Enhanced scheme of interface addressing works in conjunction with network zones and address objects. Physical interface objects include the X0, X1, X3, X4, and X5 ports in the SonicWALL security appliance.

Setup Wizard

The **Setup Wizard** button accesses the **Setup Wizard**. The Setup Wizard walks you through step-by-step the configuration of the SonicWALL security appliance for Internet connectivity.

Cross Reference: *For Setup Wizard instructions, see Chapter 48 Configuring Internet Connectivity using the Setup Wizard.*

Physical Interfaces

Physical interfaces must be assigned to a Zone to allow for configuration of Access Rules to govern inbound and outbound traffic. Security zones are bound to each physical interface where it acts as a conduit for inbound and outbound traffic. If there is no interface, traffic cannot access the zone or exit the zone.

Cross Reference: *For more information on zone, see Chapter 11 Configuring Zones.*

The first two interfaces, X0(LAN) and X1(WAN) are fixed interfaces, permanently bound to the Trusted and Untrusted Zone types. The remaining Interfaces can be configured and bound to any Zone type, depending on your SonicWALL security appliance:

- SonicWALL PRO 3060/PRO 4060/PRO5060 security appliances include four user-definable interfaces, **X2**, **X3**, **X4**, and **X5**.
- SonicWALL PRO 2040 security appliance includes two user-definable interfaces, **X2** and **X3**.
- SonicWALL TZ 170 security includes one user definable interface, **OPT**.

Note: *The Untrusted Zone type can only have two members, one of which is the fixed interface, X1.*

SonicOS Enhanced Secure Objects

The SonicOS Enhanced scheme of interface addressing works in conjunction with network zones and address objects. This structure is based on secure objects, which are utilized by rules and policies within SonicOS Enhanced. Physical interface objects include the X0, X1, X3, X4, and X5 ports in the SonicWALL security appliance linked to the LAN, WAN, DMZ, WLAN, and Custom zones. Address objects comprise a host, a network, a range of addresses, or a MAC address.

Secured objects include interface objects that are directly linked to physical interfaces and managed in the **Network>Interfaces** page. Address objects that are defined in the **Network>Objects** page. Service and Scheduling objects are defined in the **Firewall** section of the SonicWALL security appliance Management Interface, and User objects are defined in the **Users** section of the SonicWALL security appliance Management Interface.

Zones are the hierarchical apex of SonicOS Enhanced's secure objects architecture. SonicOS Enhanced includes pre-defined zones as well as allow you to define your own zones. Predefined zones include LAN, DMZ, WAN, WLAN, and Custom. Zones can include multiple interfaces, however, the WAN Zone is restricted to a total of two interfaces. Within the WAN zone, either one or both WAN interfaces can be actively passing traffic depending on the WAN Failover and Load-Balancing configuration on the **Network>WAN Failover** & LB page.

➲ **Cross Reference:** *For more information on WAN Failover and Load Balancing on the SonicWALL security appliance, see Chapter 10 Setting Up Network WAN Failover and Load Balancing.*

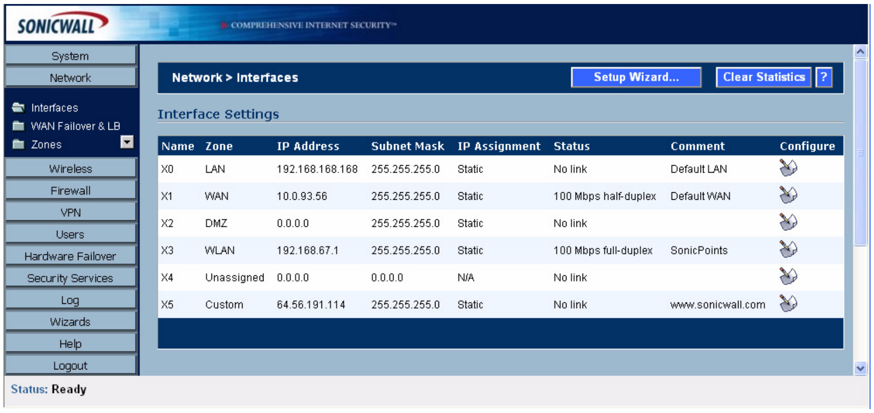
At the zone configuration level, the **Allow Interface Trust** setting for zones automates the processes involved in creating a permissive intra-zone Access Rule. It creates a comprehensive Address Object for the entire zone and a inclusively permissive Access Rule from zone address to zone addresses.

Transparent Mode

Transparent Mode in SonicOS Enhanced does not employ the concept of zones. Instead Transparent mode uses interfaces as the top level of the management hierarchy. Transparent Mode supports unique addressing and interface routing.

▲ **Alert:** *Zones are not supported in Transparent Mode.*

Interface Settings



Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	10.0.93.56	255.255.255.0	Static	100 Mbps half-duplex	Default WAN	
X2	DMZ	0.0.0.0	255.255.255.0	Static	No link		
X3	WLAN	192.168.67.1	255.255.255.0	Static	100 Mbps full-duplex	SonicPoints	
X4	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X5	Custom	64.56.191.114	255.255.255.0	Static	No link	www.sonicwall.com	

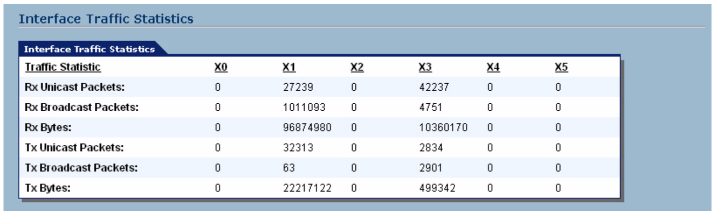
Status: Ready

The **Interface Settings** table lists the following information for each interface:

- **Name** - listed as **X0, X1**, **X2**, **X3**, **X4**, and **X5** or **LAN**, **WAN**, **WLAN**, **Custom**, or **OPT/DMZ** depending on your SonicWALL security appliance model.
- **Zone** - LAN, DMZ/OPT and WAN are listed by default. As zones are configured, the names are listed in this column.
- **IP Address** - IP address assigned to the interface.
- **Subnet Mask** - the network mask assigned to the subnet.
- **IP Assignment** - you can select from **DHCP** or **Static** for **LAN**. For **WAN**, you can select from **DHCP**, **Static**, **PPPoE**, **PPTP**, or **L2TP**.
- **Status** - the link status and speed.
- **Comment** - any user-defined comments.
- **Configure** - click the **Notepad** icon to display the **Edit Interface** window, which allows you to configure the settings for the specified interface.

Inteface Traffic Statistics

The **Interface Traffic Statistics** table lists received and transmitted information for all configured interfaces.



Traffic Statistic	X0	X1	X2	X3	X4	X5
Rx Unicast Packets:	0	27239	0	42237	0	0
Rx Broadcast Packets:	0	1011093	0	4751	0	0
Rx Bytes:	0	96874980	0	10360170	0	0
Tx Unicast Packets:	0	32313	0	2834	0	0
Tx Broadcast Packets:	0	63	0	2901	0	0
Tx Bytes:	0	22217122	0	499342	0	0

The following information is displayed for all SonicWALL security appliance interfaces:

- **Rx Unicast Packets** - indicates the number of two-way, point-to-point communications received by the interface.
- **Rx Broadcast Packets** - indicates the number of multipoint communications received by the interface.
- **RX Bytes** - indicates the volume of data, in bytes, received by the interface.
- **Tx Unicast Packets** - indicates the number of two-way, point-to-point communications received by the interface.
- **Tx Broadcast Bytes** - indicates the number of mutlipoint communications received by the interface.
- **Tx Bytes** - indicates the volume of data, in bytes, transmitted by the interface.

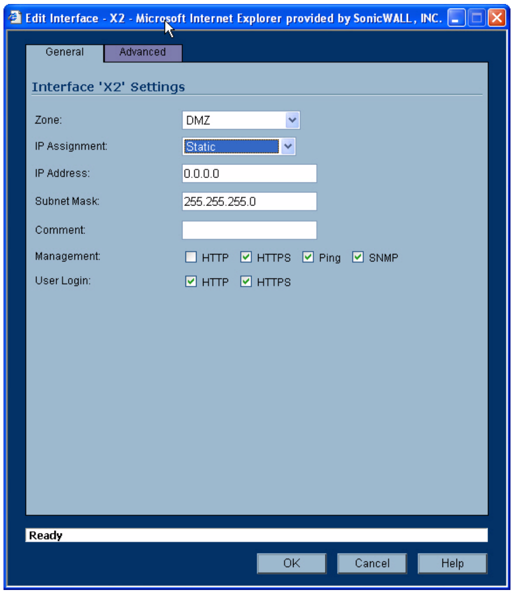
To clear the current statistics, click the **Clear Statistics** button at the top right of the **Network>Interfaces** page.

Alert: *You cannot change the Zones in the Edit Interface window for the X0 (Default LAN) and X1 (Default WAN) interfaces.*

Configuring the LAN/DMZ/Custom Interface (Static)

Static means you assign a fixed IP address to the interface.

1 Click on the **Notepad** icon in the **Configure** column for **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.


Edit Interface - X2 - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Advanced
Ready
OK
Cancel
Help

Interface 'X2' Settings

Zone: DMZ
IP Assignment: Static
IP Address: 0.0.0.0
Subnet Mask: 255.255.255.0
Comment:
Management: ☐ HTTP ☑ HTTPS ☑ Ping ☑ SNMP
User Login: ☑ HTTP ☑ HTTPS

2 Select the **LAN** interface. If you want to create a new zone for the interface, select **Create a new zone**. The **Add Zone** window is displayed. See Chapter 11 for instructions on adding a zone.

3 Select **Static** from the **IP Assignment** menu.

4 Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.

5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

6 If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **Ping**, and/or **SNMP**.

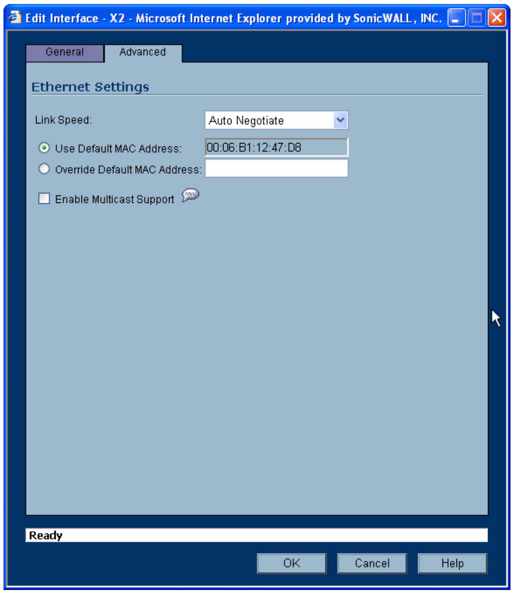
7 If you want to allow selected users with limited management rights, select **HTTP** and/or **HTTPS** in **User Login**.

8 Click **OK**.

Note: *The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance's address.*

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.


Edit Interface - X2 - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Advanced
Ethernet Settings
Ready
OK
Cancel
Help

Link Speed: Auto Negotiate

● Use Default MAC Address: 00:06:B1:12:47:D8

○ Override Default MAC Address:

☐ Enable Multicast Support

The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

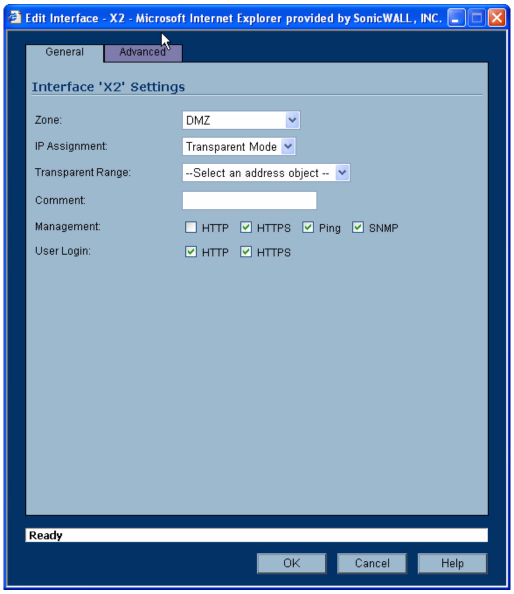
Alert: *If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.*

Configuring the LAN/DMZ/Custom Interface (Transparent Mode)

Transparent Mode enables the SonicWALL security appliance to bridge the WAN subnet onto an internal interface.

1. Click on the **Notepad** icon in the **Configure** column for **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.
2. Select the **LAN** interface. If you want to create a new zone for the interface, select **Create a new zone**. The **Add Zone** window is displayed. See Chapter 11 for instructions on adding a zone.

3 Select **Transparent Mode** from the **IP Assignment** menu.


Edit Interface - X2 - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Advanced
Ready
OK
Cancel
Help

Interface 'X2' Settings

Zone: DMZ

IP Assignment: Transparent Mode

Transparent Range: --Select an address object --

Comment:

Management: ☐ HTTP ☑ HTTPS ☑ Ping ☑ SNMP

User Login: ☑ HTTP ☑ HTTPS

4 Select the address object from the **Transparent Range** menu. See Chapter 13 for more information.

5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

6 If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **Ping**, and/or **SNMP**.

7 If you want to allow selected users with limited management rights, select **HTTP** and/or **HTTPS** in **User Login**.

8 Click **OK**.

Note: *The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance's address.*

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

Alert: *If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.*

Configuring the WLAN Interface

Static means you assign a fixed IP address to the interface.

1. Click on the **Notepad** icon in the **Configure** column for **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.
2. Select the **WLAN** interface. If you want to create a new zone for the interface, select **Create a new zone**. The **Add Zone** window is displayed. See Chapter 11 for instructions on adding a zone.
3. Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.
4. Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
5. If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **Ping**, and/or **SNMP**.
6. If you want to allow selected users with limited management rights, select **HTTP** and/or **HTTPS** in **User Login**.
7. Click **OK**.

Note: *The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance's address.*

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

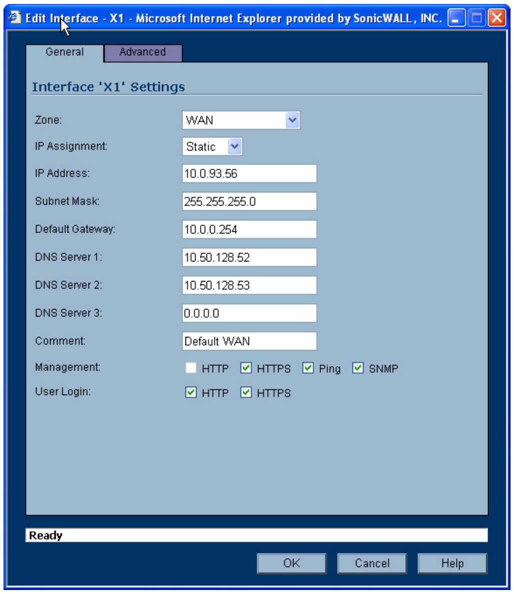
Alert: *If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.*

Configuring the WAN Interface

Configuring the WAN interface enables Internet connect connectivity. You can configure up to two WAN interfaces on the SonicWALL security appliance.

1. Click on the **Notepad** icon in the **Configure** column for the WAN or **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.

2 If you're configuring an Unassigned Interface, select **WAN** from the **Zone** menu. If you selected the **Default WAN** Interface, **WAN** is already selected in the **Zone** menu.


Edit Interface - X1 - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Advanced
Ready
OK
Cancel
Help

Interface 'X1' Settings

Zone: WAN
IP Assignment: Static
IP Address: 10.0.93.56
Subnet Mask: 255.255.255.0
Default Gateway: 10.0.0.254
DNS Server 1: 10.50.128.52
DNS Server 2: 10.50.128.53
DNS Server 3: 0.0.0.0
Comment: Default WAN
Management: ☐ HTTP ☑ HTTPS ☑ Ping ☑ SNMP
User Login: ☑ HTTP ☑ HTTPS

3 Select one of the following WAN Network Addressing Mode from the **IP Assignment** menu. Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.

Static - configures the SonicWALL for a network that uses static IP addresses.

DHCP - configures the SonicWALL to request IP settings from a DHCP server on the Internet. NAT with DHCP Client is a typical network addressing mode for cable and DSL customers.

PPPoE - uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. If desktop software and a username and password is required by your ISP, select NAT with PPPoE. This protocol is typically found when using a DSL modem.

PPTP - uses PPTP (Point to Point Tunneling Protocol) to connect to a remote server. It supports older Microsoft Windows implementations requiring tunneling connectivity.

L2TP - uses IPSec to connect a L2TP server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations. L2TP (Layer 2 Tunneling Protocol) is supported by Windows 2000 and Windows XP. If you are running other versions of Windows, you must use PPTP as your tunneling protocol.

4 After completing the WAN configuration for your Network Addressing Mode, click **OK**

Static

IP Address

Subnet Mask

Default Gateway

DNS Server 1

DNS Server 2

DNS Server 3

Comment

Management

User Login

DHCP

Host Name

Comment
Management
User Login
Renew
Release
Refresh

PPPoE

User Name
User Password
Comment
Management
User Login
Inactivity Disconnect (minutes)
Obtain IP Address Automatically
Specify IP Address
Obtain DNS Server Address Automatically
Specify DNS Server

PPTP

User Name
User Password
PPTP Server IP Address
PPTP (Client) Host Name
Comment
Management
User Login
Inactivity Disconnect (minutes)
PPTP IP Assignment
DHCP
Renew
Release
Refresh
Static
IP Address
Subnet Mask
Gateway (Router) Address

L2TP

User Name
User Password
L2TP Server IP Address
L2TP (Client) Host Name
Comment

Management

User Login

Inactivity Disconnect (minutes)

L2TP IP Assignment

DHCP

Renew

Release

Refresh

Static

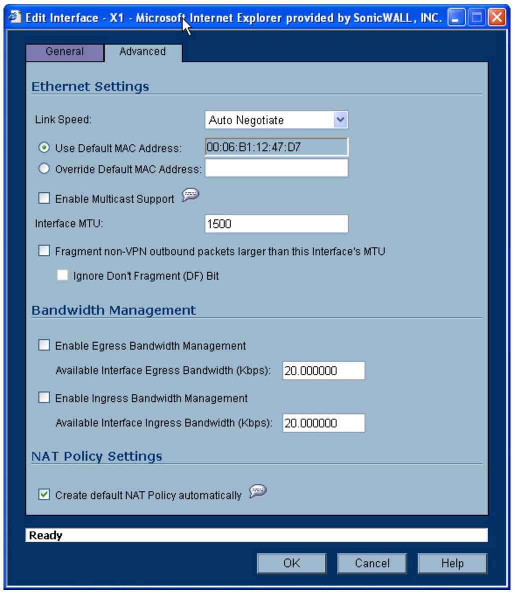
IP Address

Subnet Mask

Gateway (Router) Address

Configuring the Advanced Settings for the WAN Interface

The **Advanced** tab includes settings for forcing an Ethernet speed and duplex, overriding the Default MAC Address, setting up bandwidth management, and creating a default NAT policy automatically.


Edit Interface - X1 - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Advanced
OK
Cancel
Help

Ethernet Settings

Link Speed: Auto Negotiate

● Use Default MAC Address: 00:06:B1:12:47:D7

○ Override Default MAC Address:

☐ Enable Multicast Support

Interface MTU: 1500

☐ Fragment non-VPN outbound packets larger than this Interface's MTU

☐ Ignore Don't Fragment (DF) Bit

Bandwidth Management

☐ Enable Egress Bandwidth Management

Available Interface Egress Bandwidth (Kbps): 20.000000

☐ Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps): 20.000000

NAT Policy Settings

☑ Create default NAT Policy automatically

Ready

Ethernet Settings

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

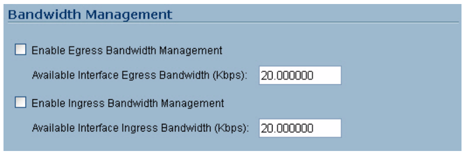
Alert: *If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.*

You can also specify any of these additional **Ethernet Settings**:

- **Interface MTU** - Specifies the largest packet size that the interface can forward without fragmenting the packet.
- **Fragment non-VPN outbound packets larger than this Interface's MT**U - Specifies all non-VPN outbound packets larger than this Interface's MTU be fragmented. Specifying the fragmenting of VPN outbound packets is set in the **VPN>Advanced** page.
- **Ignore Don't Fragment (DF) Bit** - Overrides DF bits in packets.

Bandwidth Management

SonicOS Enhanced can apply bandwidth management to both egress and ingress traffic on the WAN interface. Class Based Queuing (CBQ) provides guaranteed and maximum bandwidth Quality of Service (QoS) for the SonicWALL security appliance. Every packet destined to the WAN interface is queued in the corresponding priority queue. The scheduler then dequeues the packets and transmits it on the link depending on the guaranteed bandwidth for the flow and the available link bandwidth.



Bandwidth Management

☐ Enable Egress Bandwidth Management

Available Interface Egress Bandwidth (Kbps): 20.000000

☐ Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps): 20.000000

The **Bandwidth Management** section allows you to specify the available outbound bandwidth for this interface in Kbps.

- **Enable Egress Bandwidth Management** - Enables outbound bandwidth management.
  - **Available Interface Egress Bandwidth (Kbps)** - Specifies the available bandwidth for this interface in Kbps.
- **Enable Ingress Bandwidth Management** - Enables inbound bandwidth management.
  - **Available Interface Ingress Bandwidth (Kbps)** - Specifies the available bandwidth for this interface in Kbps.

NAT Policy Settings

Selecting **Create default NAT Policy automatically** translates the Source Address of packets from the **Default LAN** (Primary LAN) to your new **WAN** Interface.

Cross Reference: *For more information on NAT Policies, see Chapter 15 Configuring Network NAT Policies.*

CHAPTER 10

Setting Up WAN Failover and Load Balancing

Network > WAN Failover & LB

WAN Failover and Load Balancing allows you to designate one of the user-assigned interfaces as a Secondary or backup WAN port. The Secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through the Secondary WAN port if the Primary WAN port is down and/or unavailable. In this chapter, this feature is referred to as *basic failover*. This allows the SonicWALL security appliance to maintain a persistent connection for WAN port traffic by failing over to the secondary WAN port. It can also be used in a more dynamic active/active setup, where the administrator can choose a method of dividing outbound traffic flows between the Primary fixed WAN port and the user-assigned Secondary WAN port. This latter feature is referred to as *load balancing*.

WAN Failover Caveats

- WAN Failover and Load-Balancing applies to outbound-initiated traffic only; it cannot be used to perform inbound load-balancing functions, such as what a content switching or load-balancing appliance provides.
- Make sure that the SonicWALL security appliance has the proper NAT policies for the Secondary WAN interface an incorrect or missing NAT Policy for the Secondary WAN port is the most common problem seen when configuring WAN Failover & Load-Balancing.
- The Primary and Secondary WAN ports cannot be on the same IP subnet; each WAN connection must be on unique IP subnets in order to work properly

Setting Up WAN Failover and Load Balancing

The following are the steps to configuring WAN Failover and Load Balancing on the SonicWALL security appliance:

1. Configuring an interface as a Secondary WAN port
2. Creating a NAT Policy for the Secondary WAN port
3. Activating WAN Failover/Load-Balancing
4. Choosing a WAN Failover/Load-Balancing method
5. Setting Up Probe Monitoring

Configuring an Interface as a Secondary WAN Port

On **Network > Interfaces** page, configure the chosen port to be in WAN zone, and enter in the correct address settings provided by the Secondary ISP. In the example, the SonicWALL security appliance is acquiring its secondary WAN address dynamically from ISP #2, using DHCP. Any interface added to the WAN zone by default creates a NAT Policy allowing internal LAN subnets to NAT out this Secondary WAN interface.

Creating a NAT Policy for the Secondary WAN Port

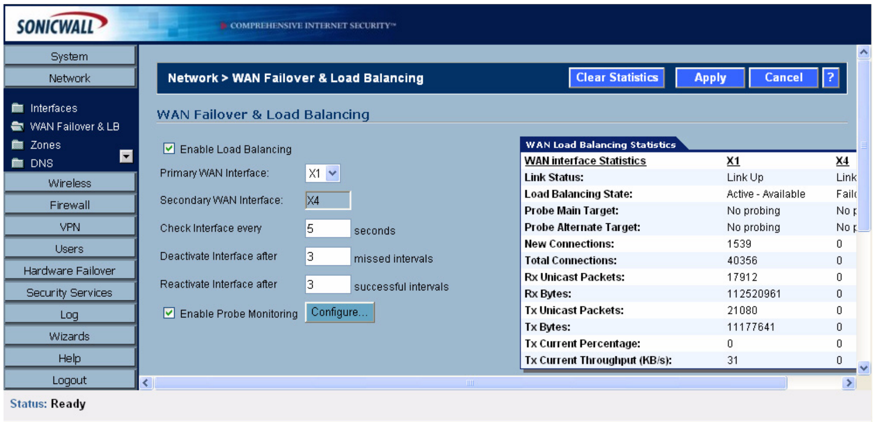
You need to create a NAT policy on your SonicWALL for WAN Failover. Follow these steps to create a NAT policy on your SonicWALL using the **X4** interface (PRO 3060/4060/PRO5060) or **OPT** interface (TZ 170):

1. Select **Network>NAT Policies**.
2. Click **Add**. The **Add NAT Policy** window is displayed.
3. Select **Any** from the **Original Source** menu.
4. Select **X4 IP** (PRO 3060/4060/5060) or **OPT IP** (TZ 170) from the **Translated Source** menu.
5. Select **Any** from the **Original Destination** menu.
6. Select **Original** from the **Translated Destination** menu.
7. Select **Any** from the **Original Service** menu.
8. Select **Original** from the **Translated Service** menu.
9. Select **X0** from the **Inbound Interface** menu.
10. Select **X4** (PRO 3060/4060/PRO5060) or **OPT** interface (TZ 170) from the **Outbound Interface** menu.
11. Make sure the **Enable** setting is checked.
12. Click **OK**.

Activating WAN Failover and Load Balancing

To configure the SonicWALL for WAN failover and load balancing, follow the steps below:

1 On **Network > WAN Failover & LB** page, select **Enable Load Balancing**.



WAN Failover & Load Balancing

☑ Enable Load Balancing

Primary WAN Interface: X1

Secondary WAN Interface: X4

Check Interface every 5 seconds

Deactivate Interface after 3 missed intervals

Reactivate Interface after 3 successful intervals

☑ Enable Probe Monitoring

WAN Load Balancing Statistics

WAN interface Statistics	X1	X4
Link Status:	Link Up	Link
Load Balancing State:	Active - Available	Fail
Probe Main Target:	No probing	No p
Probe Alternate Target:	No probing	No p
New Connections:	1539	0
Total Connections:	40356	0
Rx Unicast Packets:	17912	0
Rx Bytes:	112520961	0
Tx Unicast Packets:	21080	0
Tx Bytes:	11177641	0
Tx Current Percentage:	0	0
Tx Current Throughput (KB/s):	31	0

Status: Ready

2 From the **Secondary WAN Interface** menu, select your secondary WAN interface.

3 Enter a number between 5 and 300, in the **Check Interface Every _ Seconds** field. You can use the default value of **5** seconds

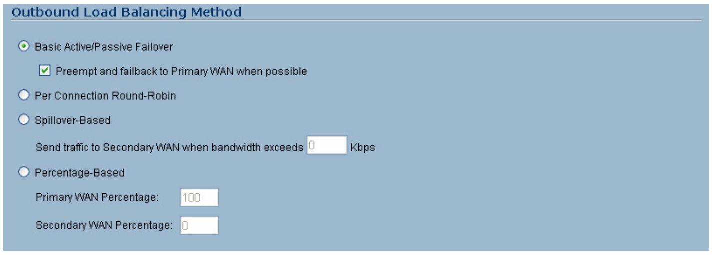
4 In the **Deactivate Interface after _ missed intervals**, enter a number between 1 and 10. You can use the default value of **3**. If the default value is used, then the interface is considered inactive after 3 successive attempts at 5 seconds each.

5 Enter a number between 1 and 10 in the **Reactivate Interface after _ successful intervals**. You can use the default value of 3. If the default value is used, then the interface is considered active after 3 successive attempts at 5 seconds each.

6 Click **Apply**.

Choosing an Outbound Load Balancing Method

You need to choose a load balancing method. By default, the SonicWALL will select **Basic Active/Passive Failover** as the method, but there are four load balancing methods available:



Outbound Load Balancing Method

● Basic Active/Passive Failover

☑ Preempt and failback to Primary WAN when possible

○ Per Connection Round-Robin

○ Spillover-Based

Send traffic to Secondary WAN when bandwidth exceeds 0 Kbps

○ Percentage-Based

Primary WAN Percentage: 100

Secondary WAN Percentage: 0

- **Basic Active/Passive Failover**: When this setting is selected, the SonicWALL security appliance only sends traffic through the Secondary WAN interface if the Primary WAN interface has been marked inactive. The SonicWALL security appliance is set to use this as the default load balancing method. If the Primary WAN fails, then the SonicWALL security appliance reverts to this method instead of the ones described below. This mode will automatically return back to using the Primary WAN interface once it has been restored (preempt mode). This item has an associated **Preempt and fail back to Primary WAN when possible** checkbox. When this checkbox is selected, the SonicWALL security appliance switches back to sending its traffic across the Primary WAN interface when it resumes responding to the SonicWALL security appliance's checks (the WAN's physical link is restored, or the logical probe targets on the WAN port resume responding).

- **Per Destination Round-Robin**: When this setting is selected, the SonicWALL security appliance load-balances outgoing traffic on a per-destination basis. This is a simple load balancing method and, though not very granular, allows you to utilize both links in a basic fashion (instead of the method above, which does not utilize the capability of the Secondary WAN until the Primary WAN has failed). The SonicWALL security appliance needs to examine outbound flows for uniqueness in source IP and destination IP and make the determination as to which interface to send the traffic out of and accept it back on. Please note this feature will be overridden by specific static route entries.
- **Spillover-Based**: When this settings is selected, the user can specify when the SonicWALL security appliance starts sending traffic through the Secondary WAN interface. This method allows you to control when and if the Secondary interface is used. This method is used if you do not want outbound traffic sent across the Secondary WAN unless the Primary WAN is overloaded. The SonicWALL security appliance has a non-Management Interface exposed hold timer set to 20 seconds – if the sustained outbound traffic across the Primary WAN interface exceeds the administrator defined Kbps, then the SonicWALL security appliance spills outbound traffic to the Secondary WAN interface (on a per-destination basis). The user entry box should not have a default entry and be left empty for the user. Please note this feature will be overridden by specific static route entries.
- **Percentage-Based**: When this setting is selected, you can specify the percentages of traffic sent through the Primary WAN and Secondary WAN interfaces. This method allows you to actively utilize both Primary and Secondary WAN interfaces. Only one entry box is required (percentage for Primary WAN), as the SonicWALL will auto-populate a non-user-editable entry box with the remaining percentage assigned to the Secondary WAN interface. Please note this feature will be overridden by specific static route entries.

Enabling WAN Probe Monitoring

If Probe Monitoring is not activated, the SonicWALL security appliance performs physical monitoring only on the Primary and Secondary WAN interfaces, meaning it only marks a WAN interface as failed if the interface is disconnected or stops receiving an Ethernet-layer signal. This is not an assured means of link monitoring, because it does not address most failure scenarios, i.e. routing issues with your ISP, or an upstream router that is no longer passing traffic. For example, if the WAN interface is connected to a hub or switch, and the router providing the connection to the ISP (also connected to this hub or switch) were to fail, the SonicWALL will continue to believe the WAN link is usable, because the connection to the hub or switch is good.

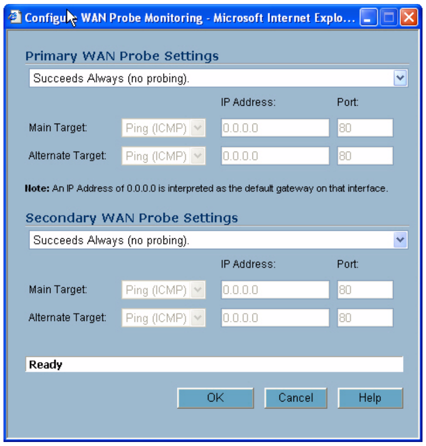
Selecting **Enabling Probe Monitoring** on **Network>WAN Failover & LB** page allows the SonicWALL security appliance to perform logical checks of upstream targets to ensure that the line is indeed usable, eliminating this potential problem, as well as continue to do physical monitoring. If Probe Monitoring is activated and the settings are left blank, the SonicWALL performs an ICMP ping probe of both WAN ports' default gateways. Unfortunately, this is also not an assured means of link monitoring, because service interruption may be occurring farther upstream. If your ISP is experiencing problems in its routing infrastructure, a successful ICMP ping of their router causes the SonicWALL security appliance to believe the line is usable, when in fact it may not be able to pass traffic to and from the public Internet at all.

To perform reliable link monitoring, you can choose ICMP or TCP as monitoring method, and can specify up to two targets for each WAN port. TCP is preferred because many devices on the public Internet now actively drop or block ICMP requests. If you specify two targets for each WAN interface, you can logically link the two probe targets such that if either one fails the line will go down, or that both must fail for the line to be considered down. Using the latter method, you can configure a sort of 'deep check' to see if the line is truly usable – for instance, you could set first probe target of your ISP's router interface using ICMP (assuming they allow this), and then do a secondary probe target of a DNS server on the public Internet using TCP Port 53. With this method, if the ICMP probe of the ISP's router fails but the farther upstream continues to respond, the SonicWALL security appliance assumes the link is usable and continue to send traffic across it.

Configuring WAN Probe Monitoring

To configure WAN probe monitoring, follow these steps:

1. On the **Network > WAN Failover & LB** page, check the **Enable Probe Monitoring** box, and click on the **Configure** button. The **Configure WAN Probe Monitoring** window is displayed.



Configu WAN Probe Monitoring - Microsoft Internet Explo...

Primary WAN Probe Settings

Succeeds Always (no probing).

		IP Address:	Port:
Main Target:	Ping (ICMP)	0.0.0.0	80
Alternate Target:	Ping (ICMP)	0.0.0.0	80

Note: An IP Address of 0.0.0.0 is interpreted as the default gateway on that interface.

Secondary WAN Probe Settings

Succeeds Always (no probing).

		IP Address:	Port:
Main Target:	Ping (ICMP)	0.0.0.0	80
Alternate Target:	Ping (ICMP)	0.0.0.0	80

Ready

2. In the **Primary WAN Probe Settings** menu, select one of the following options:

   Probe succeeds when either Main Target or Alternate Target responds.

   Probe succeeds when both Main Target and Alternative Target respond.

   Probe succeeds when Main Target responds.

   Succeeds Always (no probing).
3. Select **Ping (ICMP)** or **TCP** from the **Probe Target** menu.
4. Enter the IP address of the target device in the **IP Address** field.
5. Enter a port number in the **Port** field.
6. In the **Secondary WAN Probe Settings** menu, select one of the following options:

   Probe succeeds when either Main Target or Alternate Target responds.

   Probe succeeds when both Main Target and Alternative Target respond.

   Probe succeeds when Main Target responds.

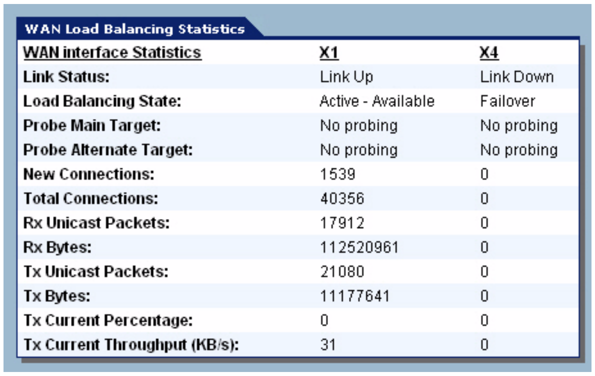
   Succeeds Always (no probing).
7. Select **Ping (ICMP)** or **TCP** from the **Probe Target** menu.
8. Enter the IP address of the target device in the **IP Address** field.
9. Enter a port number in the **Port** field.
10. Click **OK**.

Alert: *Before you begin, be sure you have configured a user-defined interface to mirror the WAN port settings.*

Note: *If the Probe Target is unable to contact the target device, the interface is deactivated and traffic is no longer sent to the primary WAN.*

WAN Load Balancing Statistics

The **WAN Load Balancing Statistics** table displays the following WAN Interface statistics for the SonicWALL:



WAN Load Balancing Statistics

WAN interface Statistics	X1	X4
Link Status:	Link Up	Link Down
Load Balancing State:	Active - Available	Failover
Probe Main Target:	No probing	No probing
Probe Alternate Target:	No probing	No probing
New Connections:	1539	0
Total Connections:	40356	0
Rx Unicast Packets:	17912	0
Rx Bytes:	112520961	0
Tx Unicast Packets:	21080	0
Tx Bytes:	11177641	0
Tx Current Percentage:	0	0
Tx Current Throughput (KB/s):	31	0

- **Link Status**
- **Load Balancing State**
- **Probe Monitoring**
- **New Connections**
- **Total Connections**
- **Rx Unicast Packets**
- **Rx Bytes**
- **Tx Unicast Packets**
- **Tx Bytes**
- **Tx Current Percentage**
- **Tx Current Throughput (KB/s)**

Click the **Clear Statistic** button on the top right of the **Network>WAN Failover & Load Balancing** page to clear information from the **WAN Load Balancing Statistics** table.

CHAPTER 11

Configuring Zones

Network > Zones

A Zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. Zone-based security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or attack.

A network security zone is simply a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Security zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.

➲ **Cross Reference:** *For more information on configuring interfaces, see Chapter 9 Configuring Interfaces.*

SonicOS Enhanced zones allows you to apply security policies to the inside of the network. This allows the administrator to do this by organizing network resources to different zones, and allowing or restricting traffic between those zones. This way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled.

Zones also allow full exposure of the NAT table to allow the administrator control over the traffic across the interfaces by controlling the source and destination addresses as traffic crosses from one zone to another. This means that NAT can be applied internally, or across VPN tunnels, which is a feature that users have long requested. SonicWALL security appliances can also drive VPN traffic through the NAT policy and zone policy, since VPNs are now logically grouped into their own VPN zone.

How Zones Work

An easy way to visualize how security zones work is to imagine a large new building, with several rooms inside the building, and a group of new employees that do not know their way around the building. This building has one or more exits, which can be thought of as the WAN interfaces. The rooms within the building have one or more doors, which can be thought of as interfaces. These rooms can be thought of as zones inside each room are a number of people. The people are categorized and assigned to separate rooms within the building. People in each room going to another room or leaving the building, must talk to a doorperson on the way out of each room. This doorperson is the inter-zone/intra-zone security policy, and the doorperson's job to consult a list and make sure that the person is allowed to go to the other room, or to leave the building. If the person is allowed (i.e. the security policy lets them), they can leave the room via the door (the interface).

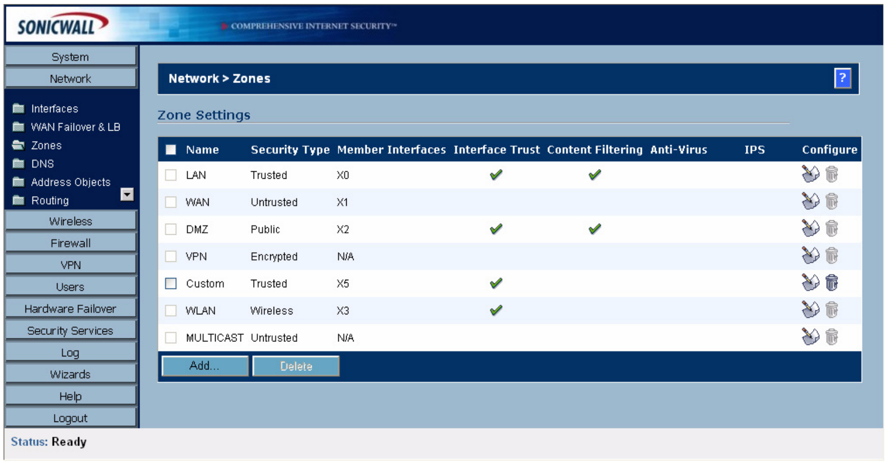
Upon entering the hallway, the person needs to consult with the hallway monitor to find out where the room is, or where the door out of the building is located. This hallway monitor provides the routing process because the monitor knows where all the rooms are located, and how to get in and out of the building. The monitor also knows the addresses of any of the remote offices, which can be considered the VPNs. If the building has more than one entrance/exit (WAN interfaces), the hallway monitor can direct people to use the secondary entrance/exit, depending upon how they've been told to do so (i.e. only in an emergency, or to distribute the traffic in and out of the entrance/exits). This function can be thought of as WAN load balancing.

There are times that the rooms inside the building have more than one door, and times when there are groups of people in the room who are not familiar with one another. In this example, one group of people uses only one door, and another group uses the other door, even though groups are all in the same room. Because they also don't recognize each other, in order to speak with someone in another group, the users must ask the doorperson (the security policy) to point out which person in the other group is the one with whom they wish to speak. The doorperson has the option to not let one group of people talk to the other groups in the room. This is an example of when zones have more than one interface bound to them, and when intra-zone traffic is not allowed.

Sometimes, people will wish to visit remote offices, and people may arrive from remote offices to visit people in specific rooms in the building. These are the VPN tunnels. The hallway and doorway monitors check to see if this is allowed or not, and allow traffic through. The doorperson can also elect to force people to put on a costume before traveling to another room, or to exit, or to another remote office. This hides the true identity of the person, masquerading the person as someone else. This process can be thought of as the NAT policy.

Predefined Zones

The predefined zones on your the SonicWALL security appliance depend on the device. The following are all the SonicWALL security appliance's predefined security zones:



Network > Zones

Zone Settings

☐	Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Anti-Virus	IPS	Configure
☐	LAN	Trusted	X0	✓	✓			
☐	WAN	Untrusted	X1					
☐	DMZ	Public	X2	✓	✓			
☐	VPN	Encrypted	N/A					
☐	Custom	Trusted	X5	✓				
☐	WLAN	Wireless	X3	✓				
☐	MULTICAST	Untrusted	N/A					

Status: Ready

The pre-defined security zones on the SonicWALL security appliance are not modifiable and are defined as follows:

- **WAN**: This zone can consist of either one or two interfaces. If you're using the security appliance's WAN failover capability, you need to add the second Internet interface to the WAN zone.
- **LAN**: This zone can consist of one to five interfaces, depending on your network design. Even though each interface will have a different network subnet attached to it, when grouped together they can be managed as a single entity.

- **DMZ**: This zone is normally used for publicly accessible servers. This zone can consist of one to four interfaces, depending on you network design.
- **VPN**: This virtual zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical interface.
- **WLAN**: This zone provides support to SonicWALL SonicPoints.
- **MULTICAST**: This zone provides support for IP multicasting, which is a method for sending IN packets from a single source simultaneously to multiple hosts.

Note: *Even though you may group interfaces together into one security zone, this does not preclude you from addressing a single interface within the Zone.*

Security Types

Each zone has a security type. The security type defines the of trust given to that zone. There are five security types:

- **Trusted**: Trusted is a security type that provides the highest level of trust--meaning that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the security appliance. The LAN zone is always Trusted.
- **Encrypted**: Encrypted is a security type used exclusively by the VPN Zone. All traffic to and from an Encrypted zone is encrypted.
- **Wireless**: Wireless is a security type applied to the WLAN zone or any zone where the only interface to the network consists of SonicWALL SonicPoint devices. You typically use WiFiSec to secure traffic in a Wireless zone. The Wireless security type is designed specifically for use with SonicPoint devices. Placing an interface in a Wireless Zone activates SDP (SonicWALL Discovery Protocol) and SSPP (SonicWALL Simple Provisioning Protocol) on that interface for automatic discovery and provisioning of SonicPoint devices. Only traffic that passes through a SonicPoint is allowed through a Wireless zone; all other traffic is dropped.
- **Public**: A Public security type offers a higher level of trust than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the security appliance and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN, but it will only have default access to the WAN, not the LAN.
- **Untrusted**: The Untrusted security type represents the lowest level of trust. It is used by both the WAN and the virtual Multicast zone. An Untrusted zone can be thought of as being on the WAN (unprotected) side of the security appliance.By default, traffic from Untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from every other zone type is permitted to Untrusted zones.

Allow Interface Trust

The **Allow Interface Trust** setting in the **Add Zone** window automates the creation of Access Rules to allow traffic to flow between the Interfaces of a zone instance. For example, if the LAN Zone has interfaces **X0**, **X3**, and **X5** assigned to it, checking **Allow Interface Trust** on the LAN Zone creates the necessary Access Rules to allow hosts on these Interfaces to communicate with each other.

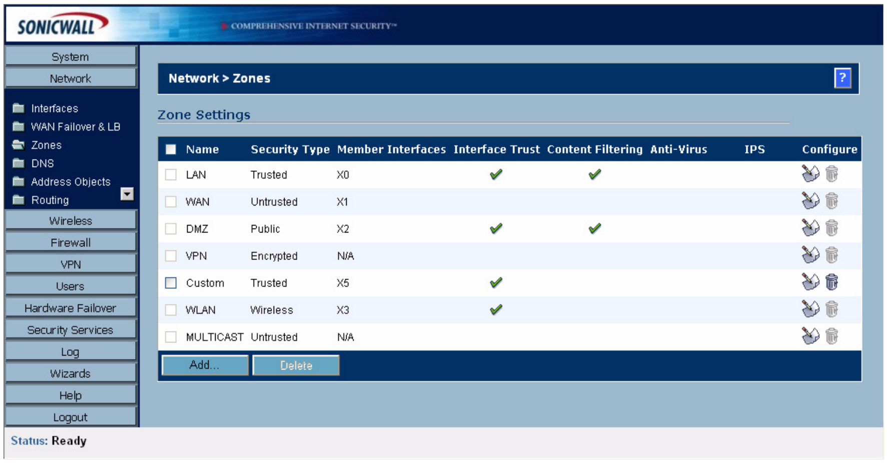
Enabling SonicWALL Security Services on Zones

You can enable SonicWALL Security Services for traffic across zones. For example, you can enable SonicWALL Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic. You can enable the following SonicWALL Security Services on zones:

- **SonicWALL Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
- **SonicWALL Enforce Anti-Virus Service** - Enforces anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **SonicWALL Intrusion Protection Service (IPS)** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.

The Zone Settings Table

The **Zone Settings** table displays a listing of all the SonicWALL security appliance default pre-defined zones as well as any zones you create. The table displays the following status information about each zone configuration:


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Interfaces
WAN Failover & LB
Zones
DNS
Address Objects
Routing
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Network > Zones
Add...
Delete
Status: Ready

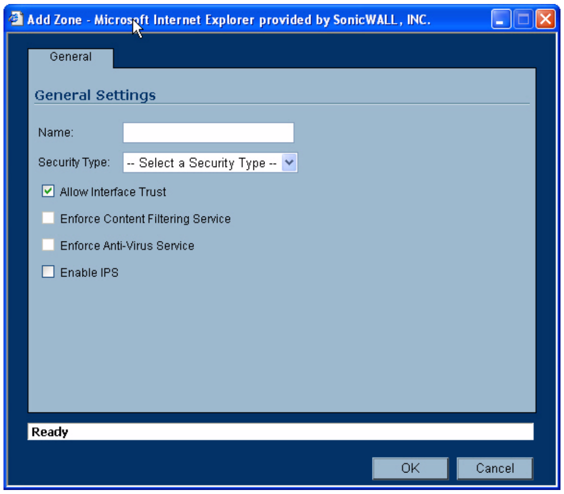
Zone Settings

☐	Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Anti-Virus	IPS	Configure
☐	LAN	Trusted	X0	✓	✓			
☐	WAN	Untrusted	X1					
☐	DMZ	Public	X2	✓	✓			
☐	VPN	Encrypted	N/A					
☐	Custom	Trusted	X5	✓				
☐	WLAN	Wireless	X3	✓				
☐	MULTICAST	Untrusted	N/A					

- **Name**: Lists the name of the zone. The predefined **LAN**, **WAN**, **WLAN**, **VPN**, and **Encrypted** zone names cannot be changed.
- **Security Type**: Displays the security type: **Trusted**, **Untrusted**, **Public**, **Wireless**, or **Encrypted**.
- **Member Interfaces**: Displays the interfaces that are members of the zone.
- **Interface Trust**: A checkmark indicates the **Allow Interface Trust** setting is enabled for the zone.
- **Content Filtering**: A checkmark indicates SonicWALL Content Filtering Service is enabled for traffic coming in and going out of the zone.
- **Anti-Virus**: A checkmark indicates SonicWALL Network Anti-Virus is enabled for traffic coming in and going out of the zone.
- **IPS**: A checkmark indicates SonicWALL Intrusion Prevention Service is enabled for traffic coming in and going out of the zone.
- **Configure**: Clicking the Notepad icon displays the Edit Zone window. Clicking the Trashcan icon deletes the zone. The Trashcan icon is dimmed for the predefined zones. You cannot delete these zones.

Adding a New Zone

To add a new Zone, click **Add** under the **Zone Settings** table. The **Add Zone** window is displayed.


Add Zone - Microsoft Internet Explorer provided by SonicWALL, INC.
General
General Settings
Ready
OK
Cancel

Name:

Security Type: -- Select a Security Type --

☑ Allow Interface Trust

☐ Enforce Content Filtering Service

☐ Enforce Anti-Virus Service

☐ Enable IPS

1. Type a name for the new zone in the **Name** field.
2. Select a security type **Trusted**, **Public** or **Wireless** from the **Security Type** menu. Use **Trusted** for Zones that you want to assign the highest level of trust, such as internal LAN segments. Use **Public** for Zones with a lower level of trust requirements, such as a DMZ Interface. Use **Wireless** for the WLAN interface.
3. If you want to allow intra-zone communications, select **Allow Interface Trust**. If not, select the **Allow Interface Trust** checkbox.
4. Select any of the SonicWALL Security Services you want to enforce on the zone.
5. Click **OK**. The new zone is now added to the SonicWALL security appliance.

Deleting a Zone

You can delete a zone by clicking the Trashcan icon in the **Configure** column. The Trashcan icon is unavailable for the predefined Zones (LAN, WAN, DMZ, VPN, WLAN, and MULTICAST). You cannot delete these zones. Any zones that you create can be deleted.

Configuring the WLAN Zone

1. Click the Edit icon for the WLAN zone. The **Edit Zone** window is displayed.
2. In the **General** tab, select the **Allow Interface Trust** setting to automate the creation of Access Rules to allow traffic to flow between the Interfaces of a zone instance. For example, if the LAN Zone has interfaces **X0**, **X3**, and **X5** assigned to it, checking **Allow Interface Trust** on the LAN Zone creates the necessary Access Rules to allow hosts on these Interfaces to communicate with each other.
3. Select any of the following settings to enable the SonicWALL Security Services on the WLAN zone:
   - **SonicWALL Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
   - **SonicWALL Enforce Anti-Virus Service** - Enforces anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
   - **SonicWALL Intrusion Protection Service (IPS)** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.

4 Click the **Wireless** tab.

5 In the **Wireless Settings** section, select **WiFiSec Enforcement** to require that all traffic that enters into the WLAN Zone interface be either IPSec traffic, WPA traffic, or both. With **WiFiSec Enforcement** enabled, all non-guest wireless clients connected to SonicPoints attached to an interface belonging to a Zone on which WiFiSec is enforced are required to use the strong security of IPSec. The VPN connection inherent in WiFiSec terminates at the “WLAN GroupVPN”, which you can configure independently of “WAN GroupVPN” or other Zone GroupVPN instances.

6 If you have enabled **WiFiSec Enforcement**, you can select **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** to require WiFiSec security for all wireless connections through the WLAN zone that are part of a site-to-site VPN.

7 Click **Trust WPA traffic as WiFiSec** to accept WPA as an allowable alternative to IPSec. Both WPA-PSK (Pre-shared key) and WPA-EAP (Extensible Authentication Protocol using an external 802.1x/EAP capable RADIUS server) will be supported on SonicPoints.

8 Under the **SonicPoint Settings** heading, select the **SonicPoint Provisioning Profile** you want to apply to all SonicPoints connected to this zone. Whenever a SonicPoint connects to this zone, it will automatically be provisioned by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings.

9 Click the **Guest Services** tab. You can choose from the following configuration options for Wireless Guest Services:

- **Enable inter-guest communication** - allows guests connecting to SonicPoints in this WLAN Zone to communicate directly and wirelessly with each other.
- **Bypass Guest Authentication** - allows a SonicPoint running WGS to integrate into environments already using some form of user-level authentication. This feature automates the WGS authentication process, allowing wireless users to reach WGS resources without requiring authentication. This feature should only be used when unrestricted WGS access is desired, or when another device upstream of the SonicPoint is enforcing authentication.
- **Enable Dynamic Address Translation (DAT)** - Wireless Guest Services (WGS) provides spur of the moment “hotspot” access to wireless-capable guests and visitors. For easy connectivity, WGS allows wireless users to authenticate and associate, obtain IP settings from the TZ 170 Wireless DHCP services, and authenticate using any web-browser. Without DAT, if a WGS user is not a DHCP client, but instead has static IP settings incompatible with the TZ 170 Wireless WLAN network settings, network connectivity is prevented until the user’s settings change to compatible values.

  Dynamic Address Translation (DAT) is a form of Network Address Translation (NAT) that allows the TZ 170 Wireless to support any IP addressing scheme for WGS users. For example, the TZ 170 Wireless WLAN interface is configured with its default address of 172.16.31.1, and one WGS client has a static IP Address of 192.168.0.10 and a default gateway of 192.168.0.1, while another has a static IP address of 10.1.1.10 and a gateway of 10.1.1.1, and DAT enables network communication for both of these clients.
- **Bypass Guest Authentication** - allows guests connecting from the device or network you select to connect without requiring guest authentication. Select the MAC address, IP Address, or subnet for which to bypass authentication.
- **Redirect SMTP traffic to** - redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
- **Deny Networks** - blocks traffic from the networks you name. Select the subnet, address group, or IP address to block traffic from.
- **Pass Networks** - automatically allows traffic through the WLAN zone from the networks you select.
- **Custom Authentication Page** - redirects users to a custom authentication page when they first connect to a SonicPoint in the WLAN zone. Click **Configure** to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click **OK**.

- **Post Authentication Page** - directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the filed.
- **Max Guests** - specifies the maximum number of guest users allowed to connect to the WLAN zone. The default is 10.

10 Click **OK** to apply these settings to the WLAN zone.

CHAPTER W

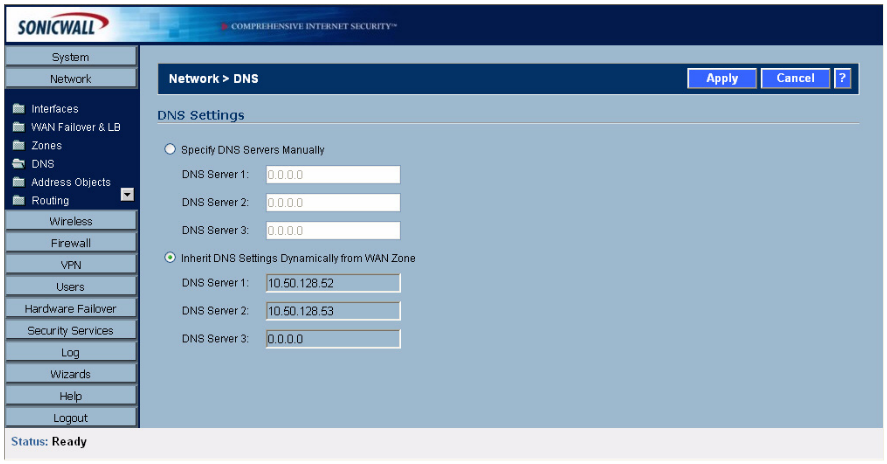
12

Configuring DNS Settings

Network > DNS

The Domain Name System (DNS) is a distributed, hierarchical system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses.

The **Network>DNS** page allows you to manually configure your DNS settings, if necessary.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Interfaces
WAN Failover & LB
Zones
DNS
Address Objects
Routing
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Network > DNS
Apply
Cancel
?

DNS Settings

○ Specify DNS Servers Manually

DNS Server 1: 0.0.0.0
DNS Server 2: 0.0.0.0
DNS Server 3: 0.0.0.0

● Inherit DNS Settings Dynamically from WAN Zone

DNS Server 1: 10.50.128.52
DNS Server 2: 10.50.128.53
DNS Server 3: 0.0.0.0

Status: Ready

In the **DNS Settings** section, select **Specify DNS Servers Manually** and enter the IP address(es) into the DNS Server fields. Click **Apply** to save your changes.

To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from the WAN Zone**. Click **Apply** to save your changes.

CHAPTER 13

Configuring Address Objects

Network > Address Objects

Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS Enhanced. These Address Objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. For example, take an internal Web-Server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, Address Objects allow you to create a single entity called "My Web Server" as a Host Address Object with an IP address of 67.115.118.80. This Address Object, "My Web Server" can then be easily and efficiently selected from a drop-down menu in any configuration screen that employs Address Objects as a defining criterion.

Types of Address Objects

Since there are multiple types of network address expressions, there are currently the following Address Objects types:

- **Host** – Host Address Objects define a single host by its IP address. The netmask for a Host Address Object will automatically be set to 32 bit (255.255.255.255) to identify it as a single host. For example, "My Web Server" with an IP address of "67.115.118.110" and a default netmask of "255.255.255.255"
- **Range** – Range Address Objects define a range of contiguous IP addresses. No netmask is associated with Range Address Objects, but internal logic generally treats each member of the specified range as a 32 bit-masked Host object. For example "My Public Servers" with an IP address starting value of "67.115.118.66" and an ending value of "67.115.118.90". All 25 individual host addresses in this range would be comprised by this Range Address Object.
- **Network** – Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network Address Objects must be defined by the network's address and a corresponding netmask. For example "My Public Network" with a Network Value of "67.115.118.64" and a Netmask of "255.255.255.224" would comprise addresses from 67.115.118.64 through to 67.115.118.95. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) are unusable.
- **MAC Address** – MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address. MAC Addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48 bit values that are expressed in 6 byte hex-notation. For

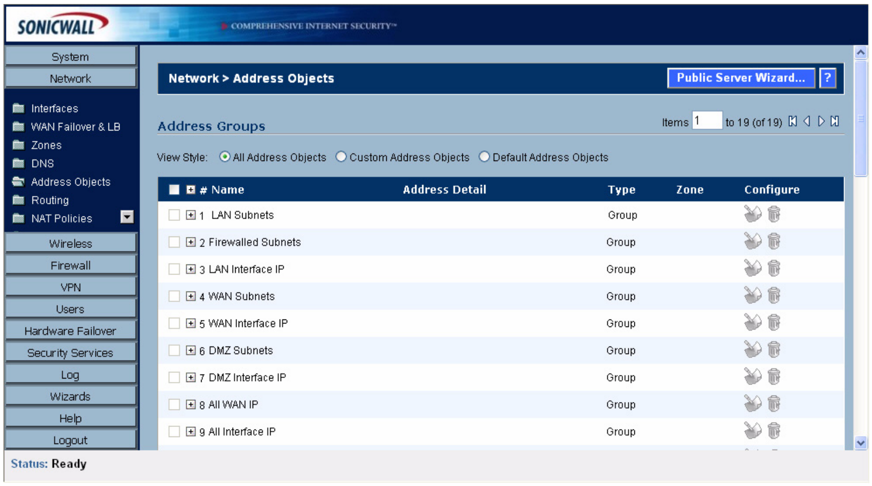
example “My Access Point” with a MAC address of “00:06:01:AB:02:CD”. MAC Address objects are used by various components of Wireless configurations throughout SonicOS.

Address Object Groups

SonicOS Enhanced also as well as the ability to group Address Objects into Address Object Groups. Groups of Address Objects can be defined to introduce further referential efficiencies. Groups can comprise any combination of Host, Range, or Network Address Objects. MAC Address Objects should be grouped separately, although they can safely be added to Groups of IP-based Address Objects, where they will be ignored when their reference is contextually irrelevant (e.g. in a NAT Policy). For example “My Public Group” can contain Host Address Object “My Web Server” and Range Address Object “My Public Servers”, effectively representing IP Addresses 67.115.118.66 to 67.115.118.90 and IP Address 67.115.118.110.

Creating and Managing Address Objects

The **Network>Address** page allows you to create and manage your Address Objects.



Address Groups

Items 1 to 19 (of 19)

View Style: ● All Address Objects ○ Custom Address Objects ○ Default Address Objects

☐	# Name	Address Detail	Type	Zone	Configure
☐	1 LAN Subnets		Group		
☐	2 Firewalled Subnets		Group		
☐	3 LAN Interface IP		Group		
☐	4 WAN Subnets		Group		
☐	5 WAN Interface IP		Group		
☐	6 DMZ Subnets		Group		
☐	7 DMZ Interface IP		Group		
☐	8 All WAN IP		Group		
☐	9 All Interface IP		Group		

Status: Ready

You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** - displays all configured Address Objects.
- **Custom Address Objects** - displays Address Objects with custom properties.
- **Default Address Objects** - displays Address Objects configured by default on the SonicWALL security appliance.

Sorting Address Objects allows you to quickly and easily locate Address Objects configured on the SonicWALL security appliance.

Note: *An Address Object must be defined before configuring NAT Policies, Access Rules, and Services.*

Navigating and Sorting the Address Objects and Address Groups Entries

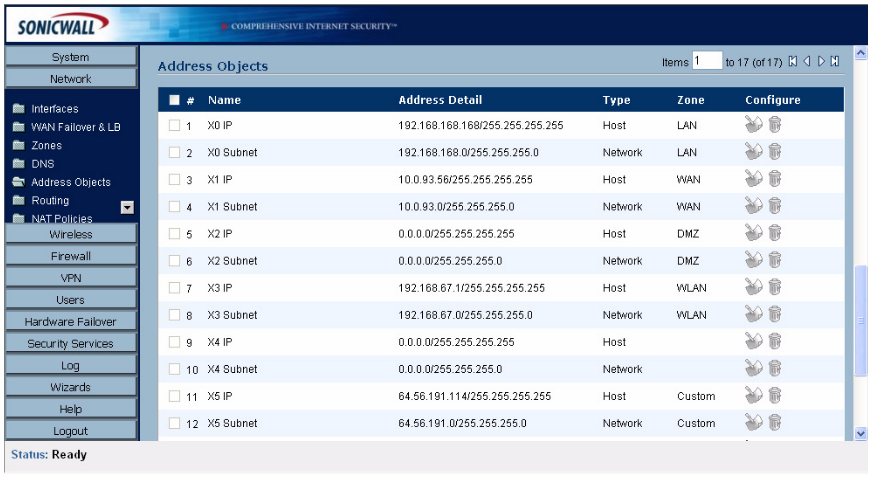
The Address Objects and Address Groups tables provides easy pagination for viewing a large number of address objects and groups. You can navigate a large number of entries listed in the Address Objects or Address Groups tables by using the navigation control bar located at the top right of the tables. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System>Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Default Address Objects and Groups

The **Default Address Objects** view displays the default **Address Objects** and **Address Groups** for your SonicWALL security appliance. The **Default Address Objects** entries cannot be modified or deleted. Therefore, the **Notepad** (Edit) and **Trashcan** (delete) icons are dimmed. The following lists the default **Address Objects** and **Address Groups** for the PRO 5060.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Interfaces
WAN Failover & LB
Zones
DNS
Address Objects
Routing
NAT Policies
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Address Objects
Items 1 to 17 (of 17)

☐	#	Name	Address Detail	Type	Zone	Configure
☐	1	X0 IP	192.168.168.168/255.255.255.255	Host	LAN	
☐	2	X0 Subnet	192.168.168.0/255.255.255.0	Network	LAN	
☐	3	X1 IP	10.0.93.56/255.255.255.255	Host	WAN	
☐	4	X1 Subnet	10.0.93.0/255.255.255.0	Network	WAN	
☐	5	X2 IP	0.0.0.0/255.255.255.255	Host	DMZ	
☐	6	X2 Subnet	0.0.0.0/255.255.255.0	Network	DMZ	
☐	7	X3 IP	192.168.67.1/255.255.255.255	Host	WLAN	
☐	8	X3 Subnet	192.168.67.0/255.255.255.0	Network	WLAN	
☐	9	X4 IP	0.0.0.0/255.255.255.255	Host		
☐	10	X4 Subnet	0.0.0.0/255.255.255.0	Network		
☐	11	X5 IP	64.56.191.114/255.255.255.255	Host	Custom	
☐	12	X5 Subnet	64.56.191.0/255.255.255.0	Network	Custom	

Status: Ready

SonicWALL PRO 5060

Default Address Objects

- X0 IP IP
- X0 Subnet
- X1 IP Host
- X1 Subnet
- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- SonicPoint

Default Address Groups

- LAN Subnets
- Firewalled Subnets
- LAN Interface IP
- WAN Subnets
- WAN Interface IP
- DMZ Subnets
- DMZ Interface IP
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- Custom Subnets
- Custom Interface IP
- All SonicPoints
- All Authorized Access Points
- WLAN Subnets
- WLAN Interface IP

SonicWALL PRO 4060

Default Address Objects

- LAN Primary IP
- LAN Primary Subnet
- WAN Primary IP
- WAN Primary Subnet
- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- WAN Remote Access Networks
- VPN DHCP Clients
- LAN Remote Access Networks
- SonicPoint

Default Address Groups

- LAN Subnets
- Firewalled Subnets
- WAN Subnets
- DMZ Subnets
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- All SonicPoints
- All Authorized Access Points
- LAN Interface IP
- WAN Interface IP
- DMZ Interface IP
- WLAN Subnets
- WLAN Interface IP
- Wireless2 Subnets
- Wireless2 Interface IP

SonicWALL PRO 3060

Default Address Objects

- LAN Primary IP
- LAN Primary Subnet
- WAN Primary IP
- WAN Primary Subnet
- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- WAN Remote Access Networks
- VPN DHCP Clients
- LAN Remote Access Networks
- SonicPoint

Default Address Groups

- LAN Subnets
- Firewalled Subnets
- WAN Subnets
- DMZ Subnets
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- All SonicPoints
- All Authorized Access Points
- LAN Interface IP
- WAN Interface IP
- DMZ Interface IP
- WLAN Subnets
- WLAN Interface IP
- Wireless2 Subnets
- Wireless2 Interface IP

SonicWALL PRO 2040

Default Address Objects

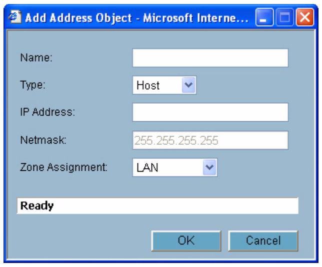
- LAN Primary IP
- LAN Primary Subnet
- WAN Primary IP
- WAN Primary Subnet
- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- WAN Remote Access Networks
- VPN DHCP Clients
- LAN Remote Access Networks
- SonicPoint

Default Address Groups

- LAN Subnets
- Firewalled Subnets
- WAN Subnets
- DMZ Subnets
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- All SonicPoints
- All Authorized Access Points
- LAN Interface IP
- WAN Interface IP
- DMZ Interface IP
- WLAN Subnets
- WLAN Interface IP
- Wireless2 Subnets
- Wireless2 Interface IP

Adding an Address Object

To add an **Address Object**, click **Add** button under the **Address Objects** table in the **All Address Objects** or **Custom Address Objects** views to display the **Add Address Object** window.



Add Address Object - Microsoft Interne...

Name:

Type: Host

IP Address:

Netmask: 255.255.255.255

Zone Assignment: LAN

Ready

1 Enter a name for the Network Object in the **Name** field.

2 Select **Host** or **Range** or **Network** from the **Type** menu.

3 If you select **Host**, enter the IP address and netmask in the **IP Address** and **Netmask** fields.

4 If you selected **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

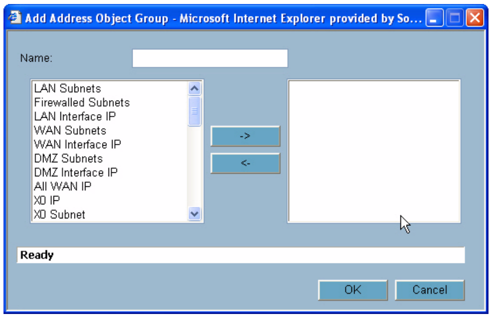
5 If you selected Network, enter the network IP address and netmask in the **Network** and **Netmask** fields.

6 Select the zone to assign to the Address Object from the **Zone Assignment** menu. You can choose **LAN, WAN**, **DMZ**, or **VPN**.

Creating Group Address Objects

As more and more Address Objects are added to the SonicWALL security appliance, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the group are applied to each address in the group.

To add a Group of Address Objects, click **Add Group** to display the **Add Address Object Group** window.

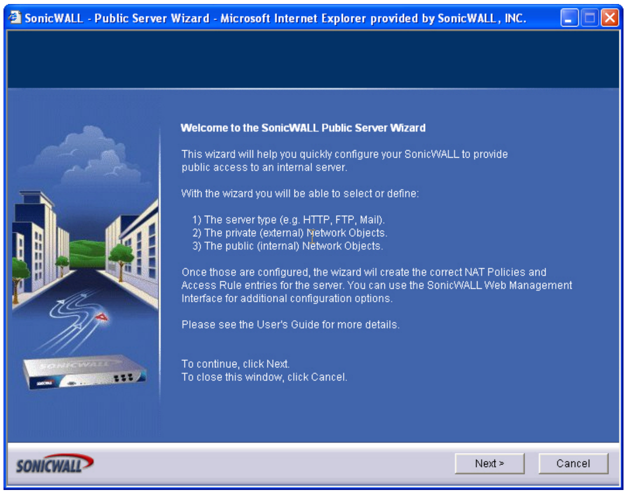

Add Address Object Group - Microsoft Internet Explorer provided by So...
Name:
LAN Subnets
Firewalled Subnets
LAN Interface IP
WAN Subnets
WAN Interface IP
DMZ Subnets
DMZ Interface IP
All WAN IP
X0 IP
X0 Subnet
->
<-
Ready
OK
Cancel

1. Create a name for the group in the **Name** field.
2. Select the Address Object from the list and click the right arrow. It is added to the group. Clicking while pressing the Ctrl key allows you to select multiple objects.
3. Click **OK**.

✓ **Tip:** *To remove an address or subnet from the group, select the IP address or subnet in the right column and click the left arrow. The selected item moves from the right column to the left column.*

Public Server Wizard

SonicOS Enhanced includes the **Public Server Wizard** to automate the process of configuring the SonicWALL security appliance for handling public servers. For example, if you have an e-mail and Web servers on your network for access from users on the Internet.


SonicWALL - Public Server Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Next >
Cancel

Welcome to the SonicWALL Public Server Wizard

This wizard will help you quickly configure your SonicWALL to provide public access to an internal server.

With the wizard you will be able to select or define:

1) The server type (e.g. HTTP, FTP, Mail).
2) The private (external) Network Objects.
3) The public (internal) Network Objects.

Once those are configured, the wizard wil create the correct NAT Policies and Access Rule entries for the server. You can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

The **Public Server Wizard** allows you to select or define the server type (HTTP, FTP, Mail), the private (external) address objects, and the public (internal) address objects. Once the server type, private and public network objects are configured, the wizard creates the correct NAT Policies and Access Rule entries on the PRO 5060 for the server. You can use the SonicWALL Management Interface for additional configuration options.

➲ **Cross Reference:** *See Part 11 Wizards for more information on configuring the SonicWALL security appliance using wizards.*

CHAPTER

14

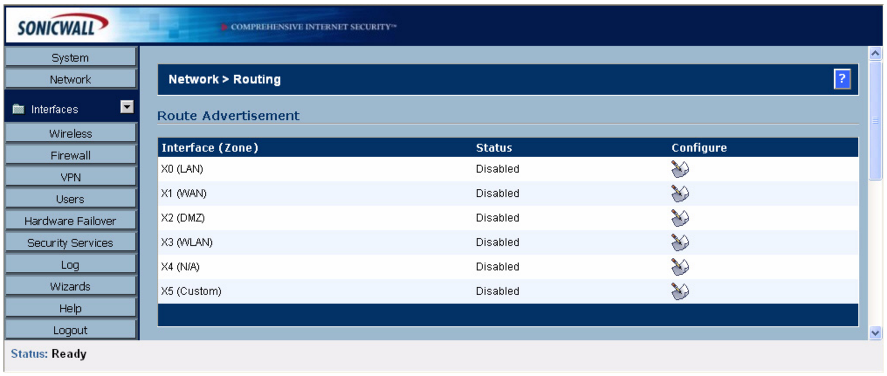
Configuring Routes

Network > Routing

If you have routers on your interfaces, you can configure static routes on the SonicWALL security appliance on the **Network>Routing** page. You can create static routing policies that create static routing entries that make decisions based upon source address, source netmask, destination address, destination netmask, service, interface, gateway and metric. This feature allows for full control of forwarding based upon a large number of user-defined variables.

Route Advertisement

The SonicWALL security appliance uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the SonicWALL security appliance and remote VPN gateways are also reflected in the RIPv2 advertisements. Choose between RIPv1 or RIPv2 based on your router's capabilities or configuration. RIPv1 is an earlier version of the protocol that has fewer features, and it also sends packets via broadcast instead of multicast. RIPv2 packets are backwards-compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection broadcasts packets instead of multicasting packets is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.



Network > Routing

Route Advertisement

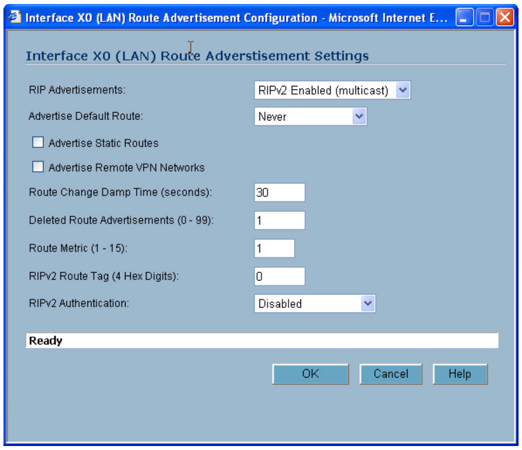
Interface (Zone)	Status	Configure
X0 (LAN)	Disabled	
X1 (WAN)	Disabled	
X2 (DMZ)	Disabled	
X3 (WLAN)	Disabled	
X4 (N/A)	Disabled	
X5 (Custom)	Disabled	

Status: **Ready**

Route Advertisement Configuration

To enable Route Advertisement for an Interface, follow these steps:

1 Click the **Notepad** icon in the **Configure** column for the interface. The **Route Advertisement Configuration** window is displayed.



Interface X0 (LAN) Route Advertisement Configuration - Microsoft Internet E...

Interface X0 (LAN) Route Adverstisement Settings

RIP Advertisements: RIPv2 Enabled (multicast)

Advertise Default Route: Never

☐ Advertise Static Routes

☐ Advertise Remote VPN Networks

Route Change Damp Time (seconds): 30

Deleted Route Advertisements (0 - 99): 1

Route Metric (1 - 15): 1

RIPv2 Route Tag (4 Hex Digits): 0

RIPv2 Authentication: Disabled

Ready

2 Select one of the following types of RIP Advertisements:

- **RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol.
- **RIPv2 Enabled (multicast)** - to send route advertisements using multicasting (a single data packet to specific notes on the network).
- **RIPv2 Enabled (broadcast)** - to send route advertisements using broadcasting (a single data packet to all nodes on the network).

3 In the **Advertise Default Route** menu, select **Never**, or **When WAN is up**, or **Always**.

4 Enable **Advertise Static Routes** if you have static routes configured on the SonicWALL security appliance, enable this feature to exclude them from Route Advertisement.

5 Enable **Advertise Remote VPN Networks** if you want to advertise VPN networks.

6 Enter a value in seconds between advertisements broadcasted over a network in the **Route Change Damp Time (seconds**) field. The default value is **30** seconds. A lower value corresponds with a higher volume of broadcast traffic over the network. The **Route Change Damp Time (seconds**) setting defines the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of temporary change in the VPN tunnel status.

7 Enter the number of advertisements that a deleted route broadcasts until it stops in the **Deleted Route Advertisements (0-99**) field. The default value is **1**.

8 Enter a value from 1 to 15 in the **Route Metric (1-15)** field. This is the number of times a packet touches a router from the source IP address to the destination IP address.

9 If RIPv2 is selected from the Route Advertisements menu, you can enter a value for the route tag in the **RIPv2 Route Tag (4 HEX Digits)** field. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements. This field is optional.

10 If you wan to enable RIPv2 authentication, select one of the following options from the **RIPv2 Authentication** menu:

- **User defined** - Enter 4 hex digits in the Authentication Type (4 hex digits) field. Enter 32 hex digits in the Authentication Data (32 Hex Digits) field.
- **Cleartext Password** - Enter a password in the Authentication Password (Max 16 Chars) field. A maximum of 16 characters can be used to define a password.

- **MD5 Digest** - Enter a numerical value from 0-255 in the Authentication Key-Id (0-255) field. Enter a 32 hex digit value for the Authentication Key (32 hex digits) field, or use the generated key.

11 Click **OK**.

Route Policies

SonicOS Enhanced provides Policy Based Routing (PBR) to to provide more flexible and granular traffic handling capabilities.

Policy Based Routing

A simple static routing entry specifies how to handle traffic that matches specific criteria, such as destination address, destination mask, gateway to forward traffic, the interface that gateway is located, and the route metric. This method of static routing satifies most static requirments, but is limited to forwarding based only on destination addressing.

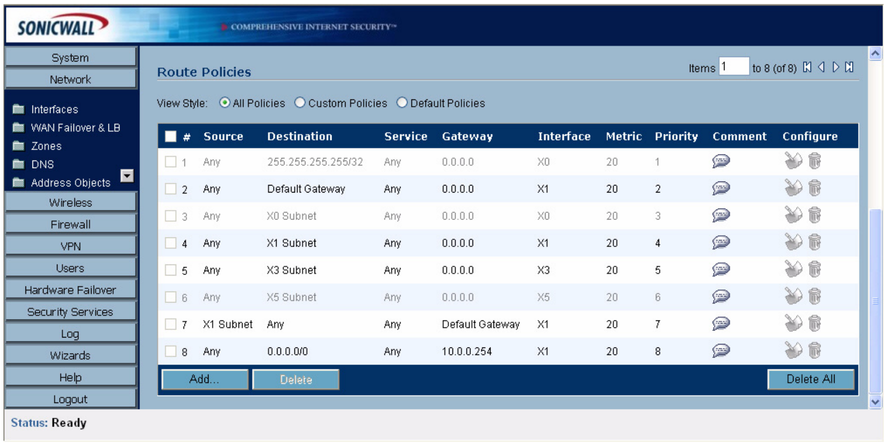
Policy Based Routing (PBR) allows you to create extended static routes to provide more flexible and granular traffic handling capabilities. SonicOS Enhanced PBR allows for matching based upon source address, source netmask, destination address, destination netmask, service, interface, and metric. This method of routing allows for full control of forwarding based upon a large number of user defined variables.

A metric is a weighted cost assigned to static and dynamic routes. Metrics have a value between 0 and 255. Lower metrics are considered better and take precedence over higher costs. SonicOS Enhanced adheres to Cisco defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

Metric Value	Description
1	Static Route
5	EIGRP Summary
20	External BGP
90	EIGRP
100	IGRP
110	OSPF
115	IS-IS
120	RIP
140	EGP
170	External EIGRP
Internal	BGP

Route Policies Table

You can change the view your route policies in the **Route Policies** table by selecting one of the view settings in the **View Style** menu.



Route Policies

Items 1 to 8 (of 8)

View Style: ● All Policies ○ Custom Policies ○ Default Policies

☐ #	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
☐ 1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1		
☐ 2	Any	Default Gateway	Any	0.0.0.0	X1	20	2		
☐ 3	Any	X0 Subnet	Any	0.0.0.0	X0	20	3		
☐ 4	Any	X1 Subnet	Any	0.0.0.0	X1	20	4		
☐ 5	Any	X3 Subnet	Any	0.0.0.0	X3	20	5		
☐ 6	Any	X5 Subnet	Any	0.0.0.0	X5	20	6		
☐ 7	X1 Subnet	Any	Any	Default Gateway	X1	20	7		
☐ 8	Any	0.0.0.0/0	Any	10.0.0.254	X1	20	8		

Status: Ready

All Policies displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **Route Policies** table provides easy pagination for viewing a large number of routing policies. You can navigate a large number of routing policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

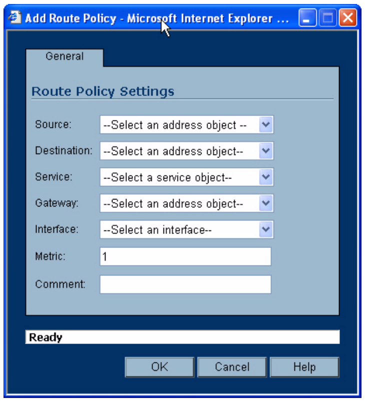
You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific routing policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System>Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

A Route Policy Example

The following example walks you through creating a route policy for two simultaneously active WAN interfaces. For this example, a secondary WAN interface needs to be setup on the X5 interface and configured with the settings from your ISP. Next, configure the PRO 5060 for load balancing by checking the **Enable Load Balancing** on the **Network>WAN Failover & LB** page. For this example, choose **Per Connection Round-Robin** as the load balancing method in the **Network>WAN Failover & LB** page. Click **Apply** to save your changes on the **Network>WAN Failover & LB** page.

1 Click the **Add** button under the Route Policies table. The **Add Route Policy** window is displayed.



Source: --Select an address object --
Destination: --Select an address object--
Service: --Select a service object--
Gateway: --Select an address object--
Interface: --Select an interface--
Metric: 1
Comment:
Ready

2 Create a routing policy that directs all **X0 Subnet** sources to **Any** destinations for **HTTP** service out of the **Default Gateway** via the **X1** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force http out primary** into the **Comment** field. Click **OK**.

3 Create a second routing policy that directs all **X0 Subnet** sources to **Any** destinations for **Telnet** service out of the **Secondary Default Gateway** via the **X5** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force telnet out backup** into the **Comment** field. Click **OK**.

These two policy-based routes force all sources from the X0 subnet to always go out the primary WAN when using any HTTP-based application, and forces all sources from the X0 subnet to always go out the backup WAN when using any Telnet-based application.

To test the HTTP policy-based route, from a computer attached to the LAN interface, access the public Web site http://www.whatismyip.com and http://whatismyip.everdot.org. Both sites display the primary WAN interface’s IP address and the secondary WAN interface.

To test the Telnet policy-based route, telnet to route-server.exodus.net and when logged in, issue the *who* command. It displays the IP address (or resolved FQDN) of the WAN IP address of the secondary WAN interface and not the primary WAN interface.

CHAPTER 15

Configuring NAT Policies

Network > NAT Policies

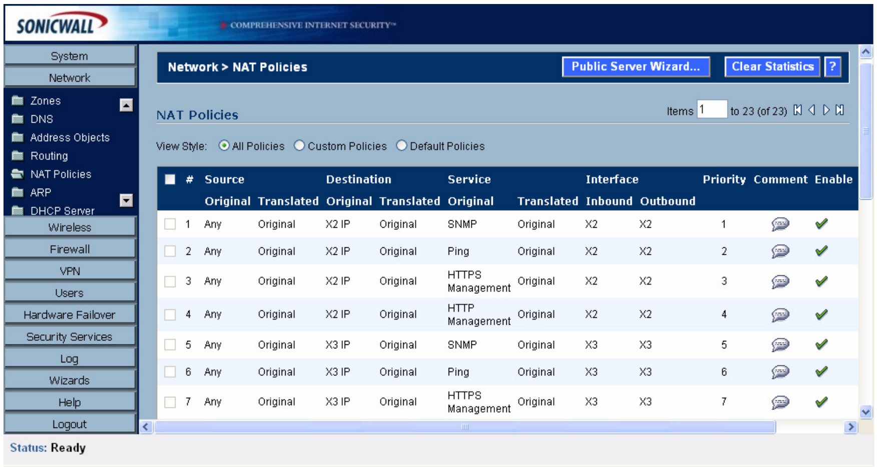
The Network Address Translation (NAT) engine in SonicOS Enhanced allows users to define granular NAT polices for their incoming and outgoing traffic. By default, the SonicWALL security appliance has a preconfigured NAT policy to allow all systems connected to the **X0** (LAN) interface to perform many-to-one NAT using the IP address of the **X1** (WAN) interface, and a policy to not perform NAT when traffic crosses between the other interfaces. This chapter explains how to set up the most common NAT policies.

Understanding how to use NAT policies starts with an the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester's IP address, the protocol information of the requestor, and the destination's IP address. The NAT Policies engine in SonicOS Enhanced can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

You can add up to 512 NAT Policies on a SonicWALL security appliance running SonicOS Enhanced, and they can be as granular as you need. It's also possible to create multiple NAT policies for the same object – for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS Enhanced supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the SonicWALL security appliance. The more granular the NAT Policy, the more precedence it takes.

NAT Policies Table

The **NAT Policies** table allows you to view your NAT Policies by **Custom Policies**, **Default Policies**, or **All Policies**.



Items 1 to 23 (of 23)

View Style: ● All Policies ○ Custom Policies ○ Default Policies

☐	#	Source		Destination		Service		Interface		Priority	Comment	Enable
		Original	Translated	Original	Translated	Original	Translated	Inbound	Outbound			
☐	1	Any	Original	X2 IP	Original	SNMP	Original	X2	X2	1	💬	✓
☐	2	Any	Original	X2 IP	Original	Ping	Original	X2	X2	2	💬	✓
☐	3	Any	Original	X2 IP	Original	HTTPS Management	Original	X2	X2	3	💬	✓
☐	4	Any	Original	X2 IP	Original	HTTP Management	Original	X2	X2	4	💬	✓
☐	5	Any	Original	X3 IP	Original	SNMP	Original	X3	X3	5	💬	✓
☐	6	Any	Original	X3 IP	Original	Ping	Original	X3	X3	6	💬	✓
☐	7	Any	Original	X3 IP	Original	HTTPS Management	Original	X3	X3	7	💬	✓

Status: Ready

▲ **Alert:** *Before configuring NAT Policies, be sure to create all Address Objects associated with the policy. For instance, if you are creating a One-to-One NAT policy, be sure you have Address Objects for your public and private IP addresses.*

✓ **Tip:** *By default, LAN to WAN has a NAT policy predefined on the SonicWALL.*

Navigating and Sorting NAT Policy Entries

You can change the view your route policies in the **NAT Policies** table by selecting one of the view settings in the **View Style** menu. **All Policies** displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **NAT Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System>Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

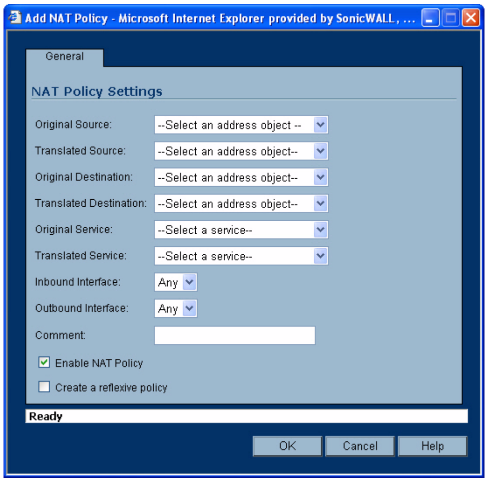
Moving your pointer over the Comment icon in the **Configure** column of **NAT Policies** table displays the comments entered in the **Comments** field of the **Add NAT Policy** window.

Moving your pointer over the Statistics icon in the **Configure** column of **NAT Policies** table displays traffic statistics for the NAT policy.

Clicking the Delete icon (trashcan) deletes the NAT Policy entry. If the icon is dimmed, the NAT Policy is a default entry and you cannot delete it.

NAT Policy Settings Explained

The following explains the settings used to create a NAT policy entry in the **Add NAT Policy** or **Edit NAT Policy** windows.


Add NAT Policy - Microsoft Internet Explorer provided by SonicWALL, ...
General
NAT Policy Settings
OK
Cancel
Help

Original Source: --Select an address object --
Translated Source: --Select an address object--
Original Destination: --Select an address object--
Translated Destination: --Select an address object--
Original Service: --Select a service--
Translated Service: --Select a service--
Inbound Interface: Any
Outbound Interface: Any
Comment:
☑ Enable NAT Policy
☐ Create a reflexive policy
Ready

Click the **Add** button in the **Network>NAT Policies** page to display the **Add NAT Policy** window to create a new NAT policy or click the Edit icon in the **Configure** column for the NAT policy you want to edit to display the **Edit NAT Policy** window.

- **Original Source**: This drop-down menu setting is used to identify the Source IP address(es) in the packet crossing the SonicWALL security appliance, whether it's across interfaces, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects. These entries can be single host entries, address ranges, or IP subnets.
- **Translated Source**: This drop-down menu setting is what the SonicWALL security appliance translates the specified **Original Source** to as it exits the SonicWALL security appliance, whether it's to another interface, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects entries. These entries can be single host entries, address ranges, or IP subnets.
- **Original Destination**: This drop-down menu setting is used to identify the Destination IP address(es) in the packet crossing the SonicWALL security appliance, whether it be across interfaces, or into/out-of VPN tunnels. When creating outbound NAT polices, this entry is usually set to **Any** since the destination of the packet is not being changed, but the source is being changed. However, these Address Object entries can be single host entries, address ranges, or IP subnets.
- **Translated Destination**: This drop-down menu setting is what the SonicWALL translates the specified **Original Destination** to as it exits the SonicWALL security appliance, whether it's to another interface, or into/out-of VPN tunnels. When creating outbound NAT polices, this entry is usually set to **Original**, since the destination of the packet is not being changed, but the source is being changed. However, these Address Objects entries can be single host entries, address ranges, or IP subnets.
- **Original Service**: This drop-down menu setting is used to identify the IP service in the packet crossing the SonicWALL security appliance, whether it's across interfaces, or into/out-of VPN tunnels. You can use the default services on the SonicWALL, or you can create your own entries. For many NAT policies, this field is set to **Any**, as the policy is only altering source or destination IP addresses.
- **Translated Service**: This drop-down menu setting is what the SonicWALL security appliance translates the **Original Service** to as it exits the SonicWALL security appliance, whether it be to another interface, or into/out-of VPN tunnels. You can use the default services in the SonicWALL

security appliance, or you can create your own entries. For many NAT Policies, this field is set to **Original**, as the policy is only altering source or destination IP addresses.

- **Inbound Interface**: This drop-down menu setting is used to specify the entry interface of the packet. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces.
- **Outbound Interface**: This drop-down is used to specify the exit interface of the packet once the NAT policy has been applied. This field is mainly used for specifying which WAN interface to apply the translation to. Of all fields in NAT policy, this one has the most potential for confusion. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces. Also, as noted in the Quick Q&A' section of this chapter, when creating inbound 1-2-1 NAT Policies where the destination is being remapped from a public IP address to a private IP address, this field must be set to **Any**.
- **Comment**: This field can be used to describe your NAT policy entry. The field has a 32-character limit, and once saved, can be viewed in the main **Network>NAT Policies** page by running the mouse over the text balloon next to the NAT policy entry. Your comment appears in a pop-up window as long as the mouse is over the text balloon.
- **Enable NAT Policy**: By default, this box is checked, meaning the new NAT policy is activated the moment it is saved. To create a NAT policy entry but not activate it immediately, uncheck this box.
- **Create a reflective policy**: When you check this box, a mirror outbound or inbound NAT policy for the NAT policy you defined in the **Add NAT Policy** window is automatically created.

NAT Policies Q&A

Why is it necessary to specify 'Any' as the destination interface for inbound 1-2-1 NAT policies?

It may seem counter-intuitive to do this, given that other types of NAT policies require you to specify the destination interface, but for this type of NAT policy, this is what is necessary. The SonicWALL security appliance uses this field during the NAT Policy lookup and validates it against the packet that it receives, but if this is set to some internal interface such as X0, the lookup fails because at that point, the SonicWALL security appliance does not know that the packet is going to X0. It's not until after the SonicWALL security appliance performs the NAT Policy lookup that it knows that the packet is going to X0. At the precise time that the SonicWALL security appliance does the NAT Policy lookup, the packet looks like it is going from X1 -> X1 (or whatever interface it is coming in on), since doing a route lookup on the NAT Public address returns the Public interface.

Can I manually order the NAT Polices?

No, the SonicWALL security appliance automatically orders them, depending on the granularity of the rule. This means that you can create NAT policy entries for the same objects, if each policy has more granularity than the existing policy. For example, you can create a NAT policy to translate all LAN systems to the WAN IP Address, then create a policy saying that a specific system on that LAN use a different IP address, and additionally, create a policy saying that specific use another IP address when using HTTP.

Can I have multiple NAT policies for the same objects?

Yes – please read the section above.

What are the NAT 'System Polices'?

On the **Network>NAT Policies** page, notice a radio button labeled **System Polices**. If you choose this radio button, the NAT Polices page displays all of the default, auto-created NAT policies for the SonicWALL security appliance. These policies are default settings for the SonicWALL security appliance to operate properly, and cannot be deleted. For this reason, they are listed in their own section, in order to make the user-created NAT policies easier to browse. If you wish to see user-created NAT policies along with the default NAT policies, simply check the radio button next to 'All Policies'.

Can I write NAT policies for VPN traffic?

Yes, this is possible if both sides of the VPN tunnel are SonicWALL security policies running SonicOS Enhanced firmware. Please refer to the technote **SonicOS Enhanced NAT VPN Overlap** for instructions on how to perform NAT on traffic entering and exiting VPN tunnels. Available at http://www.sonicwall.com/services/documentation.html.

Why do I have to write two policies for 1-2-1 traffic?

With the new NAT engine, it's necessary to write two policies – one to allow incoming requests to the destination public IP address to reach the destination private IP address (uninitiated inbound), and one to allow the source private IP address to be remapped to the source public IP address (initiated outbound). It takes a bit more work, but it's a lot more flexible.

Creating NAT Policies

NAT policies allows you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously.

For this chapter, the examples use the following IP addresses as examples to demonstrate the NAT policy creation and activation. You can use these examples to create NAT policies for your network, substituting your IP addresses for the examples shown here:

- 192.168.10.0/24 IP subnet on interface **X0**
- 67.115.118.64/27 IP subnet on interface **X1**
- 192.168.30.0/24 IP subnet on interface **X3**
- **X0** LAN IP address is 192.168.10.1
- **X1** WAN IP address is 67.115.118.68
- **X3** 'Sales' IP address is 192.168.30.1
- Webserver's "private" address at 192.168.30.200
- Webserver's "public" address at 67.115.118.70
- Public IP range addresses of 67.115.118.71 – 67.115.118.74

Creating a Many-to-One NAT Policy

Many-to-One is the most common NAT policy on a SonicWALL security appliance, and allows you to translate a group of addresses into a single address. Most of the time, this means that you're taking an internal "private" IP subnet and translating all outgoing requests into the IP address of the SonicWALL security appliance WAN port, such that the destination sees the request as coming from the IP address of the SonicWALL security appliance WAN port, and not from the internal private IP address.

This policy is easy to set up and activate. From the Management Interface, go to the **Network>NAT Policies** page and click on the **Add** button. The **Add NAT Policy** window is displayed for adding the policy. To create a NAT policy to allow all systems on the **X3** interface to initiate traffic using the SonicWALL security appliance's WAN IP address, choose the following from the drop-down boxes:

- **Original Source**: X3 Subnet

- **Translated Source**: WAN Primary IP
- **Original Destination**: Any
- **Translated Destination**: Original
- **Original Service**: Any
- **Translated Service**: Original
- **Inbound Interface**: X3
- **Outbound Interface**: X1
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. This policy can be duplicated for subnets behind the other interfaces of the SonicWALL security appliance – just replace the **Original Source** with the subnet behind that interface, adjust the source interface, and add another NAT policy.

Creating a Many-to-Many NAT Policy

The Many-to-Many NAT policy allows you to translate a group of addresses into a group of different addresses. This is useful in environments where there are an extremely high number of concurrent outgoing connections (128,000 +), as it allows the SonicWALL security appliance to utilize several addresses to perform the dynamic translation. This allows the SonicWALL security appliance to perform up to a half-million concurrent connections across the interfaces.

This policy is easy to set up and activate. You first need to go to the **Network>Address Objects** and click on the **Add** button at the bottom of the screen. When the **Add Address Object** window appears, enter in a description for the range in the **Name** field, choose **Range** from the drop-down menu, enter the range of addresses (usually public IP addresses supplied by your ISP) in the **Starting IP Address** and **Ending IP Address** fields, and select **WAN** as the zone from the **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Select **Network>NAT Policies** and click on the **Add** button. The Add NAT Policy window is displayed. To create a NAT policy to allow the systems on the LAN (X0) interface to initiate traffic using the public range addresses, choose the following from the drop-down menus:

- **Original Source**: LAN Primary Subnet
- **Translated Source**: public_range
- **Original Destination**: Any
- **Translated Destination**: Original
- **Original Service**: Any
- **Translated Service**: Original
- **Inbound Interface**: X0
- **Outbound Interface**: X1
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance dynamically maps outgoing traffic using the four available IP addresses in the range we created.

You can test the dynamic mapping by installing several systems on the LAN (X0) interface at a spread-out range of addresses (for example, 192.168.10.10, 192.168.10.100, and 192.168.10.200) and accessing the public website http://www.whatismyip.com from each system. Each system should display a different IP address from the range we created and attached to the NAT policy.

Creating a One-to-One NAT Policy for Outbound Traffic

One-to-One NAT for outbound traffic is another common NAT policy on a SonicWALL security appliance for translating an internal IP address into a unique IP address. This is useful when you need specific systems, such as servers, to use a specific IP address when they initiate traffic to other destinations. Most of the time, a NAT policy such as this one-to-one NAT policy for outbound traffic is used to map a server's private IP address to a public IP address, and it's paired with a reflective (mirror) policy that allows any system from the public Internet to access the server, along with a matching firewall access rule that permits this. Reflective NAT policies are covered in the next section.

This policy is easy to set up and activate. Select **Network>Address Objects** and click on the **Add** button at the bottom of the screen. In the **Add Address Object** window, enter a description for server's private IP address in the **Name** field. Choose Host from the **Type** menu, enter the server's private IP address in the **IP Address** field, and select the zone that the server assigned from the **Zone Assignment** menu. Click **OK**. Then, create another object in the **Add Address Object** window for the server's public IP address and with the correct values, and select **WAN** from **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Next, select **Network>NAT Policies** and click on the **Add** button to display the **Add NAT Policy** window. To create a NAT policy to allow the webserver to initiate traffic to the public Internet using its mapped public IP address, choose the following from the drop-down menus:

- **Original Source**: webserver_private_ip
- **Translated Source**: webserver_public_ip
- **Original Destination**: Any
- **Translated Destination**: Original
- **Original Service**: Any
- **Translated Service**: Original
- **Inbound Interface**: X3
- **Outbound Interface**: X1
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Checked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance translates the server's private IP address to the public IP address when it initiates traffic out the WAN (X1) interface.

You can test the one-to-one mapping by opening up a web browser on the server and accessing the public website http://www.whatismyip.com. The website should display the public IP address we attached to the private IP address in the NAT policy we just created.

Creating a One-to-One NAT Policy for Inbound Traffic (Reflective)

This is the mirror policy for the one created in the previous section when you check **Create a reflective policy**. It allows you to translate an external public IP addresses into an internal private IP address. This NAT policy, when paired with a 'permit' access policy, allows any source to connect to the internal server using the public IP address; the SonicWALL security appliance handles the translation between the private and public address. With this policy in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive via the WAN (X1) interface.

Below, you create the entry as well as the rule to allow HTTP access to the server. You need to create the access policy that allows anyone to make HTTP connections to the webserver via the webserver's public IP address.

Note: *With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.*

Go to the **Firewall>Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your server in). Click on the 'Add…' button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

- **Action**: Allow
- **Service**: HTTP
- **Source**: Any
- **Destination**: webserver_public_ip
- **Users Allowed**: All
- **Schedule**: Always on
- **Logging**: checked
- **Comment**: (enter a short description)

When you are done, attempt to access the webserver's public IP address using a system located on the public Internet. You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Inbound Port Address Translation via One-to-One NAT Policy

This type of NAT policy is useful when you want to conceal an internal server's real listening port, but provide public access to the server on a different port. In the example below, you modify the NAT policy and rule created in the previous section to allow public users to connect to the private webserver on its public IP address, but via a different port (TCP 9000), instead of the standard HTTP port (TCP 80).

First, your need to create a custom service for the different port. Go to the **Firewall>Custom Services** page and select the **Add** button. When the pop-up screen appears, give your custom service a name such as "webserver_public_port", enter in "9000" as the starting and ending port, and choose "TCP(6)" as the protocol. When done, click on the **OK** button to save the custom service.

Next, you modify the NAT policy created in the previous section that allowed any public user to connect to the webserver on its public IP address. Go to the **Network>NAT Policies** menu and click on the Edit button next to this NAT policy. The Edit NAT Policy window is displayed for editing the policy. Edit the NAT policy so that it includes the following from the drop-down menus:

- **Original Source**: Any
- **Translated Source**: Original
- **Original Destination**: webserver_public_ip
- **Translated Destination**: webserver_private_ip
- **Original Service**: webserver_public_port (or whatever you named it above)
- **Translated Service**: HTTP
- **Inbound Interface**: X1

- **Outbound Interface**: Any
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

Note: *Make sure you chose **Any** as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it's actually the correct thing to do (if you try to specify the interface, you get an error).*

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN (X1) interface, and translates the requested protocol (TCP 9000) to the server's actual listening port (TCP 80).

Finally, you're going to modify the firewall access rule created in the previous section to allow any public user to connect to the webserver on the new port (TCP 9000) instead of the server's actual listening port (TCP 80).

Note: *With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.*

Go to the **Firewall>Access Rules** section and choose the policy for the **WAN** to **Sales** zone intersection (or, whatever zone you put your server in). Click on the **Configure** button to bring up the previously created policy. When the pop-up appears, edit in the following values:

- **Action**: Allow
- **Service**: webserver_public_port (or whatever you named it above)
- **Source**: Any
- **Destination**: webserver_public_ip
- **Users Allowed**: All
- **Schedule**: Always on
- **Logging**: checked
- **Comment**: (enter a short description)

When you're done, attempt to access the webserver's public IP address using a system located on the public Internet on the new custom port (example: http://67.115.118.70:9000). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Inbound Port Address Translation via WAN (X1) IP Address

This is one of the more complex NAT policies you can create on a SonicWALL security appliance running SonicOS Enhanced – it allows you to use the WAN IP address of the SonicWALL security appliance to provide access to multiple internal servers. This is most useful in situations where your ISP has only provided a single public IP address, and that IP address has to be used by the SonicWALL security appliance's WAN interface.

Below, you create the programming to provide public access to two internal webservers via the SonicWALL security appliances WAN IP address; each is tied to a unique custom port. In the following examples, you set up two, but it's possible to create more than these as long as the ports are all unique.

In this section, we have five tasks to complete:

1. Create two custom service objects for the unique public ports the servers respond on.

2 Create two address objects for the servers' private IP addresses.

3 Create two NAT entries to allow the two servers to initiate traffic to the public Internet.

4 Create two NAT entries to map the custom ports to the actual listening ports, and to map the private IP addresses to the SonicWALL's WAN IP address.

5 Create two access rule entries to allow any public user to connect to both servers via the SonicWALL's WAN IP address and the servers' respective unique custom ports.

First, you need to create a custom service for the different port. Go to the Firewall>Custom Services page and click on the Add button. When the pop-up screen appears, give your custom services names such as "servone_public_port" and "servtwo_public_port", enter in "9100" and "9200" as the starting and ending port, and choose "TCP(6)" as the protocol. When done, click on the **OK** button to save the custom services.

Second, to go to the **Network>Address Objects** and click on the **Add** button at the bottom of the page. In the **Add Address Objects** window, enter in a description for server's private IP addresses, choose 'Host' from the drop-down box, enter the server's private IP addresses, and select the zone that the servers are in. When done, click on the 'OK' button to create the range object.

Third, from the SonicWALL's management GUI, go to the **Network>NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create a NAT policy to allow the two servers to initiate traffic to the public Internet using the SonicWALL security appliance's WAN IP address, choose the following from the drop-down boxes:

- **Original Source**: servone_private_ip
- **Translated Source**: WAN Primary IP
- **Original Destination**: Any
- **Translated Destination**: Original
- **Original Service**: Any
- **Translated Service**: Original
- **Inbound Interface**: X3
- **Outbound Interface**: X1
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

And:

- **Original Source**: servtwo_private_ip
- **Translated Source**: WAN Primary IP
- **Original Destination**: Any
- **Translated Destination**: Original
- **Original Service**: Any
- **Translated Service**: Original
- **Inbound Interface**: X3
- **Outbound Interface**: X1
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

When done, click on the **OK** button to add and activate the NAT policies. With these policies in place, the SonicWALL security appliance translates the servers' private IP addresses to the public IP address when it initiates traffic out the WAN (X1) interface.

Fourth, go to the **Network>NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create the NAT policies to map the custom ports to the servers' real listening ports and to map the SonicWALL's WAN IP address to the servers' private addresses, choose the following from the drop-down boxes:

- **Original Source**: Any
- **Translated Source**: Original
- **Original Destination**: WAN Primary IP
- **Translated Destination**: servone_private_ip
- **Original Service**: servone_public_port
- **Translated Service**: HTTP
- **Inbound Interface**: X1
- **Outbound Interface**: Any
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

And:

- **Original Source**: Any
- **Translated Source**: Original
- **Original Destination**: WAN Primary IP
- **Translated Destination**: servtwo_private_ip
- **Original Service**: servtwo_public_port
- **Translated Service**: HTTP
- **Source Interface**: X1
- **Destination Interface**: Any
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

Note: *Make sure you choose 'Any' as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it's actually the correct thing to do (if you try to specify the interface, you get an error).*

When done, click on the 'OK' button to add and activate the NAT policies. With these policies in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN (X1) interface.

Fifth, you need to create the access rules that allows anyone from the public Internet to access the two webservers using the custom ports and the SonicWALL security appliance's WAN IP address.

Note: *With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS 2.0 Enhanced. If you write a rule to the private IP address, the rule does not work.*

Go to the **Firewall>Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your serves in). Click on the 'Add…' button to bring up the pop-up window to create the policies. When the pop-up appears, enter the following values:

- **Action**: Allow
- **Service**: servone_public_port (or whatever you named it above)
- **Source**: Any
- **Destination**: X1 IP Address
- **Users Allowed**: All
- **Schedule**: Always on
- **Logging**: checked
- **Comment**: (enter a short description)

And:

- **Action**: Allow
- **Service**: servtwo_public_port (or whatever you named it above)
- **Source**: Any
- **Destination**: X1 IP Address
- **Users Allowed**: All
- **Schedule**: Always on
- **Logging**: checked
- **Comment**: (enter a short description)

When you're done, attempt to access the webservers via the SonicWALL's WAN IP address using a system located on the public Internet on the new custom port (example: http://67.115.118.70:9100 and http://67.115.118.70:9200). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

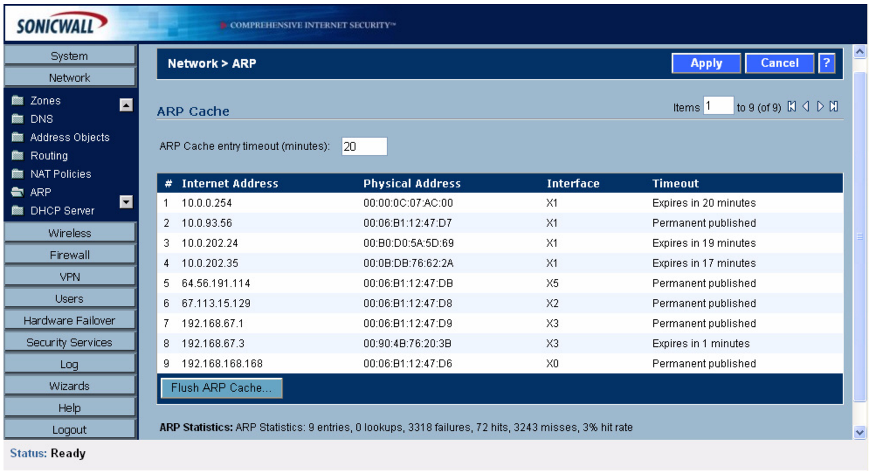
CHAPTER

16

Managing ARP Traffic

Network > ARP

ARP (Address Resolution Protocol) maps layer 3 (IP addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. ARP is a broadcast protocol that can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Zones
DNS
Address Objects
Routing
NAT Policies
ARP
DHCP Server
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Network > ARP
Apply
Cancel
?
ARP Cache
Flush ARP Cache...
Status: Ready

Items 1 to 9 (of 9)

ARP Cache entry timeout (minutes): 20

#	Internet Address	Physical Address	Interface	Timeout
1	10.0.0.254	00:00:0C:07:AC:00	X1	Expires in 20 minutes
2	10.0.93.56	00:06:B1:12:47:D7	X1	Permanent published
3	10.0.202.24	00:B0:D0:5A:5D:69	X1	Expires in 19 minutes
4	10.0.202.35	00:0B:DB:76:62:2A	X1	Expires in 17 minutes
5	64.56.191.114	00:06:B1:12:47:DB	X5	Permanent published
6	67.113.15.129	00:06:B1:12:47:D8	X2	Permanent published
7	192.168.67.1	00:06:B1:12:47:D9	X3	Permanent published
8	192.168.67.3	00:90:4B:76:20:3B	X3	Expires in 1 minutes
9	192.168.168.168	00:06:B1:12:47:D6	X0	Permanent published

ARP Statistics: ARP Statistics: 9 entries, 0 lookups, 3318 failures, 72 hits, 3243 misses, 3% hit rate

Navigating and Sorting the ARP Cache Table Entries

The **ARP Cache** tabe table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System>Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Flushing the ARP Cache

It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. Since the IP address is linked to a physical address, the IP address can change but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache. Click **Flush ARP** Cache to clear the information.

To configure a specific length of time for the entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field.

CHAPTER 17

Setting Up the DHCP Server

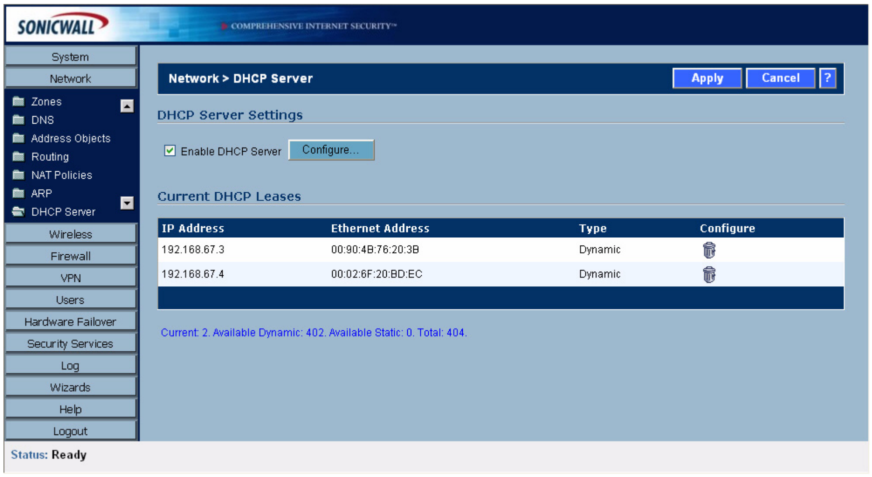
Network > DHCP Server

The SonicWALL security appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. The **Network>DHCP Server** page includes settings for configuring the SonicWALL security appliance's DHCP server.

You can use the SonicWALL security appliance's DHCP server or use existing DHCP servers on your network. If your network uses its own DHCP servers, make sure the **Enable DHCP Server** checkbox is unchecked.

Enabling DHCP Server

If you want to use the SonicWALL security appliance's DHCP server, select **Enable DHCP Server**, and click **Configure** on the **Network>DHCP Server** page.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Zones
DNS
Address Objects
Routing
NAT Policies
ARP
DHCP Server
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Network > DHCP Server
Apply
Cancel
?
Configure...

DHCP Server Settings

☑ Enable DHCP Server

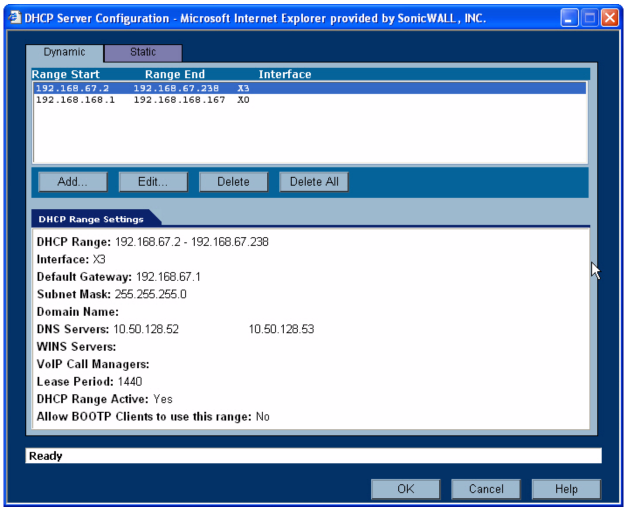
Current DHCP Leases

IP Address	Ethernet Address	Type	Configure
192.168.67.3	00:90:4B:76:20:3B	Dynamic	🗑
192.168.67.4	00:02:6F:20:BD:EC	Dynamic	🗑

Current: 2. Available Dynamic: 402. Available Static: 0. Total: 404.

Status: Ready

The **DHCP Server Configuration** window is displayed. In the **Dynamic Ranges** table, the **Range Start**, **Range End**, and **Interface** information is displayed.


DHCP Server Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
Dynamic
Static
Add...
Edit...
Delete
Delete All
DHCP Range Settings
OK
Cancel
Help

Range Start	Range End	Interface
192.168.67.2	192.168.67.238	X3
192.168.168.1	192.168.168.167	X0

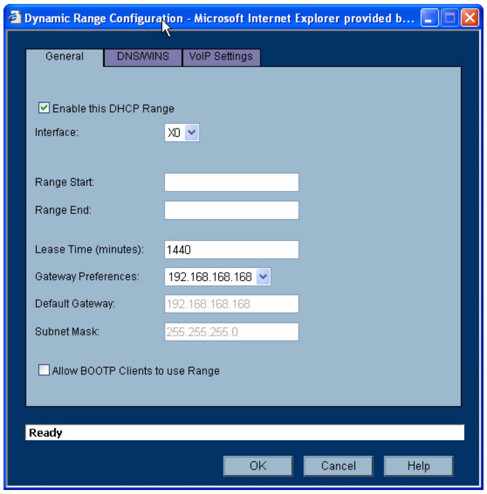
DHCP Range: 192.168.67.2 - 192.168.67.238
Interface: X3
Default Gateway: 192.168.67.1
Subnet Mask: 255.255.255.0
Domain Name:
DNS Servers: 10.50.128.52 10.50.128.53
WINS Servers:
VoIP Call Managers:
Lease Period: 1440
DHCP Range Active: Yes
Allow BOOTP Clients to use this range: No

Ready

Configuring DHCP Server for Dynamic Ranges

To configure DHCP server for dynamic IP address ranges, follow these instructions:

1. In the **Dynamic** page, click **Add**. The **Dynamic Ranges Configuration** window is displayed.


Dynamic Range Configuration - Microsoft Internet Explorer provided b...
General
DNS/WINS
VoIP Settings
OK
Cancel
Help

☑ Enable this DHCP Range
Interface: X0
Range Start:
Range End:
Lease Time (minutes): 1440
Gateway Preferences: 192.168.168.168
Default Gateway: 192.168.168.168
Subnet Mask: 255.255.255.0
☐ Allow BOOTP Clients to use Range

Ready

General

1. In the **General** page, make sure the **Enable this DHCP Range** is checked, if you want to enable this range.
2. Select the interface from the Interface menu. The IP addresses are in the same private subnet as the selected interface.

✓ **Tip:** *To select an interface from the Interface menu, it must first be fully configured and it must be of the Zone type, LAN or DMZ.*

3. Use the default IP address range entries for the interface in the **Range Start** and **Range End** fields or type in your own IP address range.
4. Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.
5. Select the gateway from the **Gateway Preferences** menu. The interface IP address is the default value, but you can select **Other** and type a different IP address for the gateway.

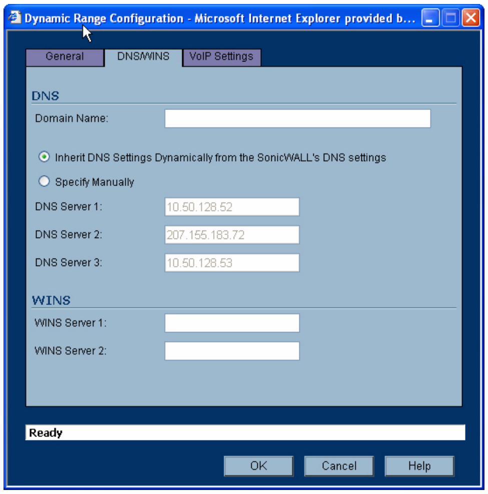
6 If you select the interface IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to type the **Default Gateway** and **Subnet Mask** information into the fields.

7 Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

BOOTP stands for bootstrap protocol, which is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a BOOTP server.

DNS/WINS

1 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.



Dynamic Range Configuration - Microsoft Internet Explorer provided b...

General | DNS/WINS | VoIP Settings

DNS

Domain Name:

● Inherit DNS Settings Dynamically from the SonicWALL's DNS settings

○ Specify Manually

DNS Server 1: 10.50.128.52

DNS Server 2: 207.155.183.72

DNS Server 3: 10.50.128.53

WINS

WINS Server 1:

WINS Server 2:

Ready

2 If you have a domain name for the DNS server, type it in the **Domain Name** field.

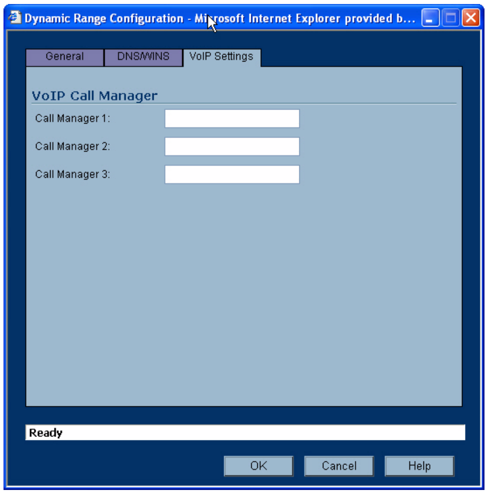
3 **Inherit DNS Settings Dynamically using SonicWALL's DNS Settings** is selected by default.

4 If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

5 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can add an additional WINS server.

VoIP Settings

1 .Click on the **VoIP Settings** tab. The **VoIP Settings** tab allows you to configure the SonicWALL DHCP server to send Cisco Call Manager information to VoIP clients on the network.



Dynamic Range Configuration - Microsoft Internet Explorer provided b...

General | DNS/WINS | VoIP Settings

VoIP Call Manager

Call Manager 1:

Call Manager 2:

Call Manager 3:

Ready

2 Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager** 1 field. You can add two additional VoIP Call Manager addresses.

3 Click **OK** to add the settings to the SonicWALL security appliance.

4 Click **Apply** for the settings to take effect on the SonicWALL security appliance.

Cross Reference: *For more information on VoIP support features on the SonicWALL security appliance, see Chapter 28 Configuring VoIP Support.*

Configuring Static DHCP Entries

Click the **Static** tab to add static DHCP entries to the SonicWALL security appliance. Static entries are IP addresses assigned to servers requiring permanent IP settings.

Note: *Static DHCP entries should not be configured for computers with IP addresses configured in Network*

To configure static entries, follow these steps:

1 In the **Static** page of the **DHCP Server Configuration** window, click **Add**. The **Static Entry Configuration** window is displayed.

General

1 In the **General** tab, make sure the **Enable this DHCP Entry** is checked, if you want to enable this range.

2 Select the interface from the Interface menu. The IP addresses are in the same private subnet as the selected interface.

3 Type the device IP address in the **Static IP Address** field.

4 Type the device Ethernet (MAC) address in the **Ethernet Address** field.

5 Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.

6 Select the gateway from the **Gateway Preferences** menu. The interface IP address is the default value, but you can select **Other** and type a different IP address for the gateway.

7 If you select the SonicWALL security appliance LAN IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to type the **Default Gateway** and nformation into the fields.

DNS/WINS

1 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.

2 If you have a domain name for the DNS Server, type it in the **Domain Name** field.

3 **Inherit DNS Settings Dynamically from the SonicWALL's DNS settings** is selected by default. When selected, the DNS Server IP fields are unavailable.

4 If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

5 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can specify an additional WINS server.

VoIP Settings

1 Click on the **VoIP Settings** tab. The **VoIP Settings** tab allows you to configure the SonicWALL DHCP server to send Cisco Call Manager information to VoIP clients on the network.

2 Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager** 1 field. You can add two additional VoIP Call Manager addresses.

3. Click **OK** to add the settings to the SonicWALL.
4. Click **Apply** for the settings to take effect on the SonicWALL.

✓ **Tip:** *The SonicWALL DHCP server can assign a total of 64 address ranges with 64 IP addresses each or a total of 4096 IP addresses.*

For more information on VoIP support features on the SonicWALL security appliance, see Chapter 28 Configuring VoIP Support.

Current DHCP Leases

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding displays the IP address and the Ethernet address along with the type of binding, Dynamic, Dynamic BOOTP, or Static BOOTP. To delete a binding, which frees the IP address on the DHCP server, click the Trashcan icon next to the entry. To edit an entry, click the Notepad icon for the entry.

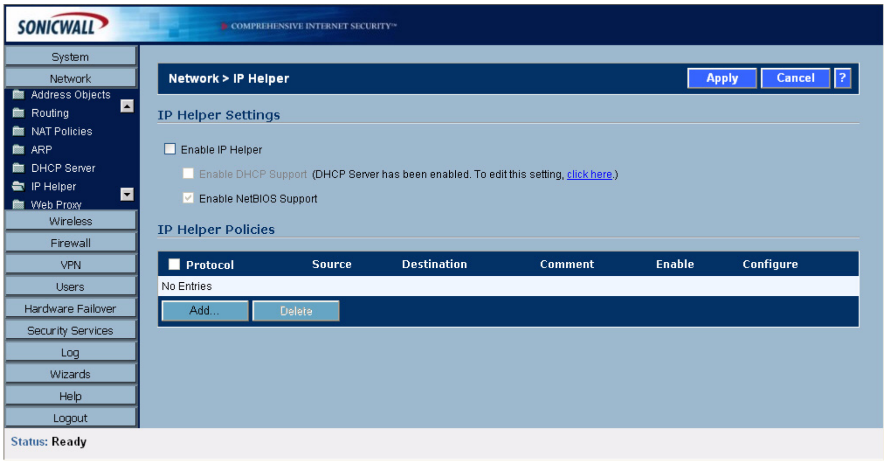
CHAPTER

18

Using IP Helper

Network > IP Helper

The IP Helper allows the SonicWALL security appliance to forward DHCP requests originating from the interfaces on a SonicWALL security appliance to a centralized DHCP server on the behalf of the requesting client. IP Helper is used extensively in routed VLAN environments where a DHCP server is not available for each interface, or where the layer 3 routing mechanism is not capable of acting as a DHCP server itself. The IP Helper also allows NetBIOS broadcasts to be forwarded with DHCP client requests.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Address Objects
Routing
NAT Policies
ARP
DHCP Server
IP Helper
Web Proxy
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Network > IP Helper
Apply
Cancel
?
Add...
Delete

IP Helper Settings

☐ Enable IP Helper

☐ Enable DHCP Support (DHCP Server has been enabled. To edit this setting, click here.)

☑ Enable NetBIOS Support

IP Helper Policies

☐ Protocol	Source	Destination	Comment	Enable	Configure
No Entries					

Status: Ready

IP Helper Settings

- **Enable IP Helper -** enables IP Helper features.
- **Enable DHCP Support** - enables DHCP forwarding from the SonicWALL security appliance to your central DHCP server. If the DHCP server has been enabled, the message "**DHCP Server has been enabled. To edit this setting, click here.**" is displayed. Clicking the link displays the **Network>DHCP Server** page.
- **Enable NetBIOS Support** - enables NetBIOS broadcast forwarding with the DHCP requests. NetBIOS is required to allow Windows operating systems to browse for resources on a network.

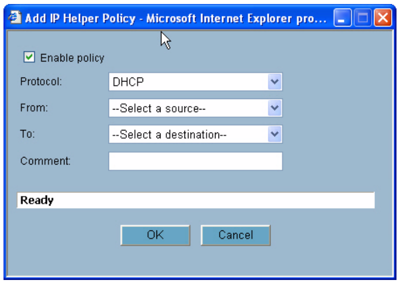
▲ **Alert:** *The SonicWALL DHCP Server feature must be disabled before you can enable DHCP Support.*

IP Helper Policies

IP Helper Policies allow you to forward DHCP and NetBIOS broadcasts from one interface to another interface.

Adding an IP Helper Policy

1. Click the **Add** button under the **IP Helper Policies** table. The **Add IP Helper Policy** window is displayed.



☑ Enable policy
Protocol: DHCP
From: --Select a source--
To: --Select a destination--
Comment:
Ready

2. The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.
3. Select **DHCP** or **NetBIOS** from the **Protocol** menu.
4. Select a source Interface or Zone from the **From** menu.
5. Select a destination IP address or subnet from the **To** menu or select **Create a new network** to create a new **Address Object**.
6. Enter an optional comment in the **Comment** field.
7. Click **OK** to add the policy to the **IP Helper Policies** table.

Editing an IP Helper Policy

Click the **Notepad** icon in the **Configure** column of the **IP Helper Policies** table to display the **Edit IP Helper** window, which includes the same settings as the **Add IP Helper Policy** window.

Deleting IP Helper Policies

Click the Trashcan icon to delete the individual IP Helper policy entry.

Click the **Delete** button to delete all the selected IP Helper policies in the **IP Helper Policies** table.

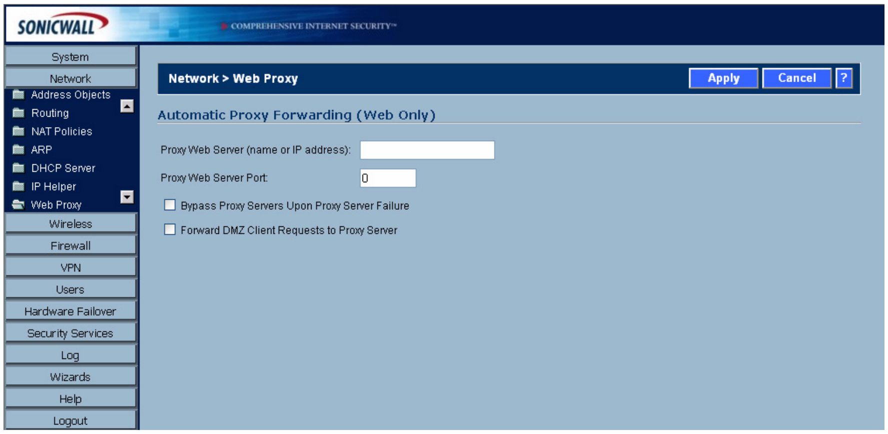
CHAPTER 19

Setting Up Web Proxy Forwarding

Network > Web Proxy

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests. Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

If you have a proxy server on your network, instead of configuring each computer's Web browser to point to the proxy server, you can move the server to the WAN and enable Web Proxy Forwarding using the settings on the **Network>Web Proxy** page. The SonicWALL security appliance automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the network to be configured.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Address Objects
Routing
NAT Policies
ARP
DHCP Server
IP Helper
Web Proxy
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Network > Web Proxy
Apply
Cancel
?

Automatic Proxy Forwarding (Web Only)

Proxy Web Server (name or IP address):

Proxy Web Server Port: 0

☐ Bypass Proxy Servers Upon Proxy Server Failure

☐ Forward DMZ Client Requests to Proxy Server

Configuring Automatic Proxy Forwarding (Web Only)

▲ **Alert:** *The proxy server must be located on the WAN; it can not be located on the LAN.*

To configure a Proxy Web sever, select the **Network>Web Proxy** page.

1 Connect your Web proxy server to a hub, and connect the hub to the SonicWALL security appliance WAN port.

2. Type the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.
3. Type the proxy IP port in the **Proxy Web Server Port** field.
4. To bypass the Proxy Servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.
5. Select **Forward DMZ Client Requests to Proxy Server** if you have clients configured on the DMZ.
6. Click **Apply**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

Bypass Proxy Servers Upon Proxy Failure

If a Web proxy server is specified on the **Firewall>Web Proxy** page, selecting the **Bypass Proxy Servers Upon Proxy Server Failure** check box allows clients behind the SonicWALL security appliance to bypass the Web proxy server in the event it becomes unavailable. Instead, the client's browser accesses the Internet directly as if a Web proxy server is not specified.

PART

4

Wireless

:

CHAPTER

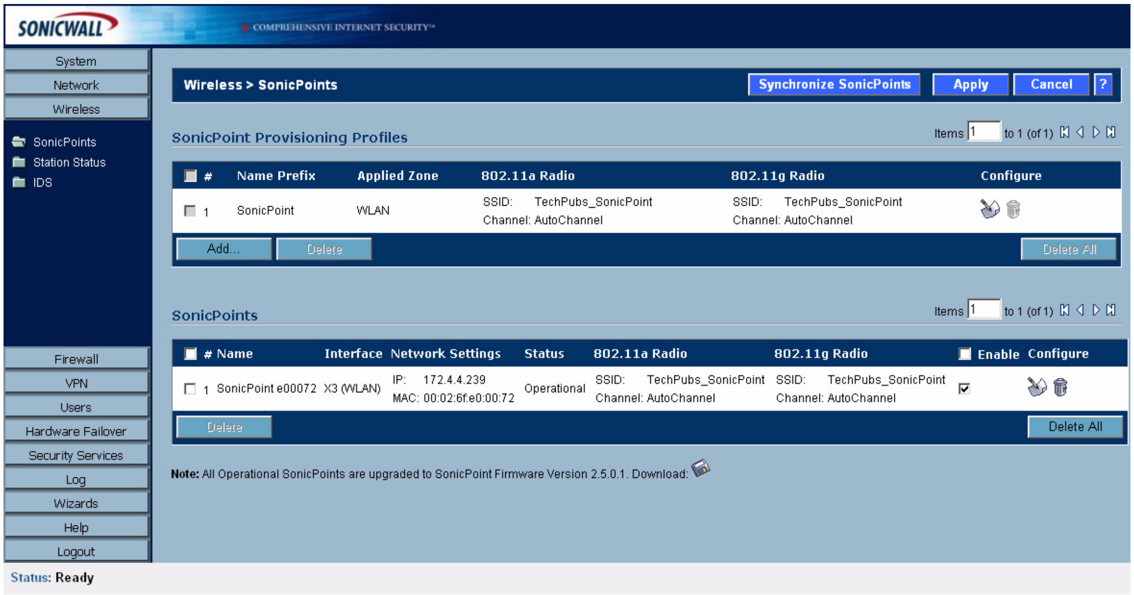
20

Managing SonicPoints

Wireless > SonicPoints

SonicWALL SonicPoints are wireless access points specially engineered to work with SonicWALL security appliances running SonicOS Enhanced 2.5 or greater to provide wireless access throughout your enterprise.

The Wireless section of the Management Interface lets you manage the SonicPoints connected to your system.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
SonicPoints
Station Status
IDS
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Wireless > SonicPoints
Synchronize SonicPoints
Apply
Cancel
?
Items 1 to 1 (of 1)
Add...
Delete
Delete All

SonicPoint Provisioning Profiles

☐ #	Name Prefix	Applied Zone	802.11a Radio	802.11g Radio	Configure
☐ 1	SonicPoint	WLAN	SSID: TechPubs_SonicPoint Channel: AutoChannel	SSID: TechPubs_SonicPoint Channel: AutoChannel	

SonicPoints

☐ #	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	☐ Enable	Configure
☐ 1	SonicPoint e00072	X3 (WLAN)	IP: 172.4.4.239 MAC: 00:02:6f:e0:00:72	Operational	SSID: TechPubs_SonicPoint Channel: AutoChannel	SSID: TechPubs_SonicPoint Channel: AutoChannel	☑	

Note: All Operational SonicPoints are upgraded to SonicPoint Firmware Version 2.5.0.1. Download:

Status: Ready

Before Managing SonicPoints

Before you can manage SonicPoints in the Management Interface, you must first:

- Configure your SonicPoint Provisioning Profiles
- Configure a Wireless zone.
- Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.

- Assign one or more interfaces to the Wireless zone.
- Attach the SonicPoints to the interfaces in the Wireless zone.
- Test SonicPoints

SonicPoint Provisioning Profiles

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSID's, and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. Any profile can apply to any number of zones. Then, when a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

SonicOS includes a default SonicPoint profile, named SonicPoint. You can modify this profile or create a new one.

The default SonicPoint profile has the following settings:

802.11a Radio		**802.11g Radio**	
Enable 802.11a Radio	Yes	**Enable 802.11g Radio**	Yes
SSID	SonicWALL	**SSID**	SonicWALL
Radio Mode	54Mbps - 802.11a	**Radio Mode**	2.4 GHz 54Mbps - 802.11g
ACL Enforcement	Disabled	**ACL Enforcement**	Disabled
Authentication Type	WEP - Both Open System & Shared Key	**Authentication Type**	WEP - Both Open System & Shared Key
Data Rate	Best	**Data Rate**	Best
Antenna Diversity	Best	**Antenna Diversity**	Best

Configuring a SonicPoint Profile

You can add any number of SonicPoint profiles. To configure a SonicPoint provisioning profile:

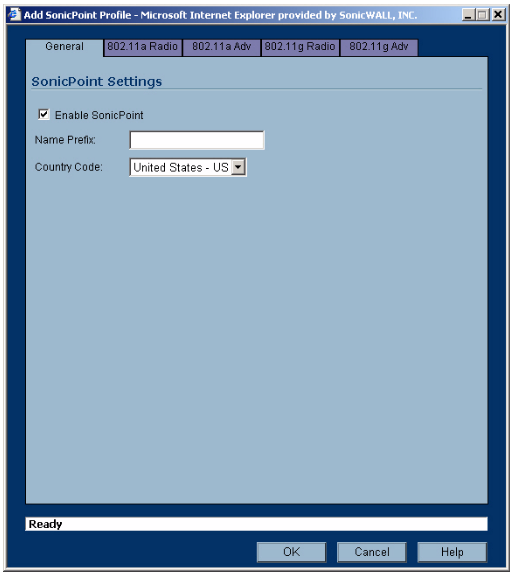
1 To add a new profile click **Add** below the list of SonicPoint provisioning profiles

To edit an existing profile, select the profile and click the edit icon in the same line as the profile you are editing.

2 In the **General** tab of the Add Profile window, specify:

- **Enable SonicPoint**: Check this to automatically enable each SonicPoint when it is provisioned with this profile.
- **Name Prefix**: Enter a prefix for the names of all SonicPoints connected to this zone. When each SonicPoint is provisioned it is given a name that consists of the name prefix and a unique number, for example: “SonicPoint 126008.“

- **Country Code**: Select the country where you are operating the SonicPoints. The country code determines which regulatory domain the radio operation falls under.


Add SonicPoint Profile - Microsoft Internet Explorer provided by SonicWALL, INC.
General
802.11a Radio
802.11a Adv
802.11g Radio
802.11g Adv
OK
Cancel
Help

SonicPoint Settings

☑ Enable SonicPoint

Name Prefix:

Country Code: United States - US

Ready

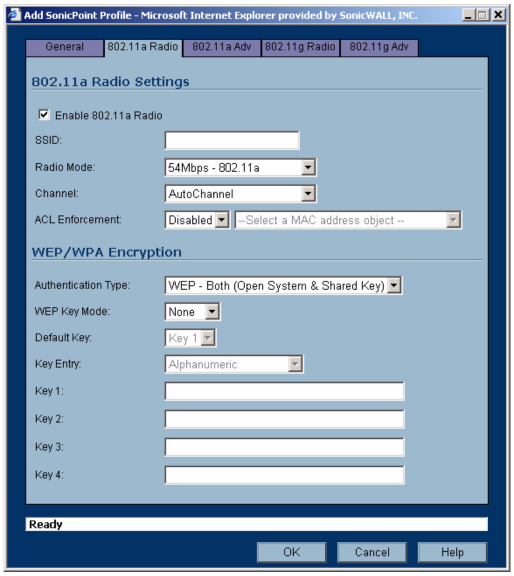
3 In the **802.11a** tab, Configure the radio settings for the 802.11a (5GHz band) radio:

- **Enable 802.11a Radio**: Check this to automatically enable the 802.11a radio bands on all SonicPoints provisioned with this profile.
- **SSID**: Enter a recognizable string for the SSID of each SonicPoint using this profile. This is the name that will appear in clients’ lists of available wireless connections.

Note: *If all SonicPoints in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint to another.*

- **Radio Mode**: Select the speed of the wireless connection. You can choose **54 Mbps** or **108 Mbps (Turbo)** mode. If you choose Turbo mode, all users in your company must use wireless access cards from the same manufacturer.
- **Channel**: Select the channel the radio will operate on. The default is **AutoChannel**, which automatically selects the channel with the least interference. Use AutoChannel unless you have a specific reason to use or avoid specific channels.
- **ACL Enforcement**: Select this to enforce Access Control by allowing or denying traffic from specific devices. Select an address object from the list of
- **Authentication Type**: Select the method of authentication for your wireless network. You can select **WEP - Both (Open System & Shared Key)**, **WEP - Open System**, **WEP - Shared Key**, **WPA - PSK**, or **WPA - EAP**.
- **WEP Key Mode**: Select the size of the encryption key.
- **Default Key**: Select which key in the list below is the default key, which will be tried first when trying to authenticate a user.
- **Key Entry**: Select whether the key is alphanumeric or hexadecimal.

- **Key 1 - Key 4**: Enter the encryptions keys for WEP encryption. Enter the most likely to be used in the field you selected as the default key.


Add SonicPoint Profile - Microsoft Internet Explorer provided by SonicWALL, INC.
General
802.11a Radio
802.11a Adv
802.11g Radio
802.11g Adv
Ready
OK
Cancel
Help

802.11a Radio Settings

☑ Enable 802.11a Radio

SSID:

Radio Mode: 54Mbps - 802.11a

Channel: AutoChannel

ACL Enforcement: Disabled --Select a MAC address object --

WEP/WPA Encryption

Authentication Type: WEP - Both (Open System & Shared Key)

WEP Key Mode: None

Default Key: Key 1

Key Entry: Alphanumeric

Key 1:

Key 2:

Key 3:

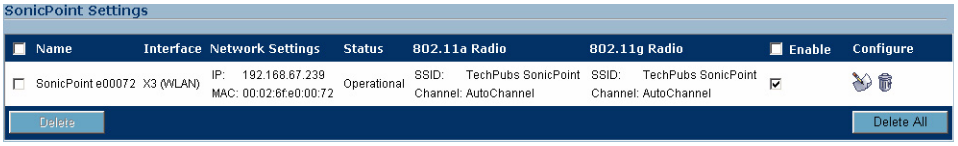
Key 4:

4. In the **802.11a Advanced** tab, configure the performance settings for the 802.11a radio. For most 802.11a advanced options, the default settings give optimum performance.
    - **Hide SSID in Beacon**: Check this option to have the SSID broadcast as part of the wireless beacon, rather than as a separate broadcast.
    - **Data Rate**: Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. You can select: **Best**, **6 Mbps**, **9 Mbps**, **12 Mbps**, **18 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps**, or **54 Mbps**.
    - Transmit Power: Select the transmission power. Transmission power effects the range of the SonicPoint. You can select: **Full Power**, **Half (-3 dB)**, **Quarter (-6 dB)**, **Eighth (-9 dB)**, or **Minimum**.
    - **Antenna Diversity**: Select whether you want to use both antennas, one antenna, or have the SonicPoint automatically select the best setup for the situation.
    - **Beacon Interval (milliseconds)**: Enter the number of milliseconds between sending out a wireless beacon.
    - **DTIM Interval**: Enter the interval in milliseconds.
    - **Fragmentation Threshold (bytes)**: Enter the number of bytes of fragmented data you want the network to allow.
    - **RTS Threshold (bytes)**: Enter the number of bytes.
    - **Maximum Client Associations**: Enter the maximum number of clients you want the SonicPoint to support on this radio at one time.
5. Configure the settings in the **802.11g Radio** and **802.11g Advanced** tabs. These settings affect the operation of the 802.11g radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both the 802.11a and 802.11g bands at the same time.

    The settings in the **802.11g Radio** and **802.11g Advanced** tabs are similar to the settings in the **802.11a Radio** and **802.11a Advanced** tabs. Follow the instructions in step 3 and step 4 in this procedure to configure the 802.11g radio.

When a SonicPoint unit is first connected and powered up, it will have a factory default configuration (IP Address 192.168.1.20, username: admin, password: password). Upon initializing, it will attempt to find a SonicOS device with which to peer. If it is unable to find a peer SonicOS device, it will enter into a stand-alone mode of operation with a separate stand-alone configuration allowing it to operate as a standard Access Point.

If the SonicPoint does locate, or is located by a peer SonicOS device, via the SonicWALL Discovery Protocol, an encrypted exchange between the two units will ensue wherein the profile assigned to the relevant Wireless Zone will be used to automatically configure (provision) the newly added SonicPoint unit.

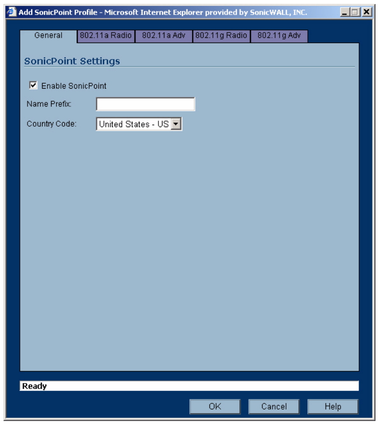


SonicPoint Settings

☐ Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	☐ Enable	Configure
☐ SonicPoint e00072	X3 (WLAN)	IP: 192.168.67.239 MAC: 00:02:6f:e0:00:72	Operational	SSID: TechPubs SonicPoint Channel: AutoChannel	SSID: TechPubs SonicPoint Channel: AutoChannel	☑	

Delete
Delete All

As part of the provisioning process, SonicOS will assign the discovered SonicPoint device a unique name, and it will record its MAC address and the interface and Zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS will then use the profile associated with the relevant Zone to configure the 2.4GHz and 5GHz radio settings.



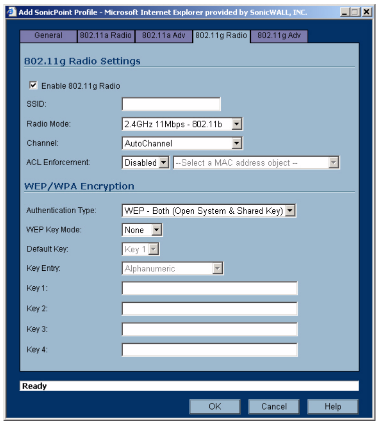
Add SonicPoint Profile - Microsoft Internet Explorer provided by SonicWALL, INC.
General
802.11a Radio
802.11a Adv
802.11g Radio
802.11g Adv
Ready
OK
Cancel
Help

SonicPoint Settings

☑ Enable SonicPoint

Name Prefix:

Country Code: United States - US



Add SonicPoint Profile - Microsoft Internet Explorer provided by SonicWALL, INC.
General
802.11a Radio
802.11a Adv
802.11g Radio
802.11g Adv
Ready
OK
Cancel
Help

802.11g Radio Settings

☑ Enable 802.11g Radio

SSID:

Radio Mode: 2.4GHz 11Mbps - 802.11b

Channel: AutoChannel

ACL Enforcement: Disabled --Select a MAC address object --

WEP/WPA Encryption

Authentication Type: WEP - Both (Open System & Shared Key)

WEP Key Mode: None

Default Key: Key 1

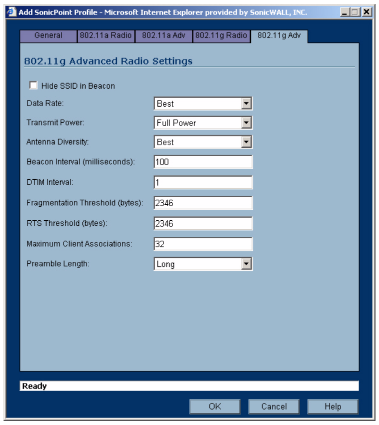
Key Entry: Alphanumeric

Key 1:

Key 2:

Key 3:

Key 4:



Add SonicPoint Profile - Microsoft Internet Explorer provided by SonicWALL, INC.
General
802.11a Radio
802.11a Adv
802.11g Radio
802.11g Adv
Ready
OK
Cancel
Help

802.11g Advanced Radio Settings

☐ Hide SSID in Beacon

Data Rate: Best

Transmit Power: Full Power

Antenna Diversity: Best

Beacon Interval (milliseconds): 100

DTIM Interval: 1

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2346

Maximum Client Associations: 32

Preamble Length: Long

Modifications to profiles will not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:

- Via manual configuration changes – Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its Zone.
- Via un-provisioning – Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it will automatically engage the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a Zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a *controlled* fashion, rather than changing all peered SonicPoints at once, which can cause service disruptions.

Updating SonicPoint Settings

You can change the settings of any individual SonicPoint liste on the Wireless > SonicPoints page.

Edit SonicPoint settings

To edit the settings of an individual SonicPoint:

1. Under SonicPoint Settings, click the Edit icon ✎ in the same line as the SonicPoint you want to edit.
2. In Edit SonicPoint screen, make the changes you want. The Edit SonicPoint screen has the following tabs:
   - **General**

- **802.11a Radio**
- **802.11a Advanced**
- **802.11g Radio**
- **802.11g Advanced**

The options on these tabs are the same as the Add SonicPoint Profile screen. See **Configuring a SonicPoint Profile** for instructions on configuring these settings.

3 Click **OK** to apply these settings.

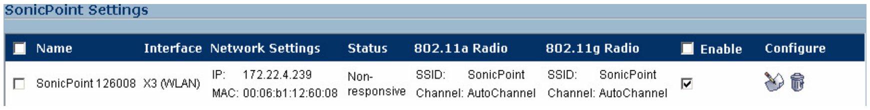
Synchronize SonicPoints

Click **Synchronize SonicPoints** at the top of the Wireless > SonicPoints page to update the settings for each SonicPoint reported on the page. When you click **Synchronize SonicPoints**, SonicOS polls all connected SonicPoints and displays updated settings on the page.

Enable and Disable Individual SonicPoints

You can enable or disable individual SonicPoints on the Wireless > SonicPoints page:

1 Check the box under Enable to enable the SonicPoint, uncheck the box to disable it.



SonicPoint Settings

☐ Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	☐ Enable	Configure
☐ SonicPoint 126008	X3 (WLAN)	IP: 172.22.4.239 MAC: 00:06:b1:12:60:08	Non-responsive	SSID: SonicPoint Channel: AutoChannel	SSID: SonicPoint Channel: AutoChannel	☑	

2 Click Click **Apply** at the top of the Wireless > SonicPoints page to apply this setting to the SonicPoint.

Updating SonicPoint Firmware

SonicOS Enhanced 2.5 (or greater) contains an image of the SonicPoint firmware. When you connect a SonicPoint to a security appliance runnign SonicOS Enhanced 2.5 (or greater), the appliance checks the version of the SonicPoint's firmware, and automatically updates it, if necessary.

Automatic Provisioning (SDP & SSPP)

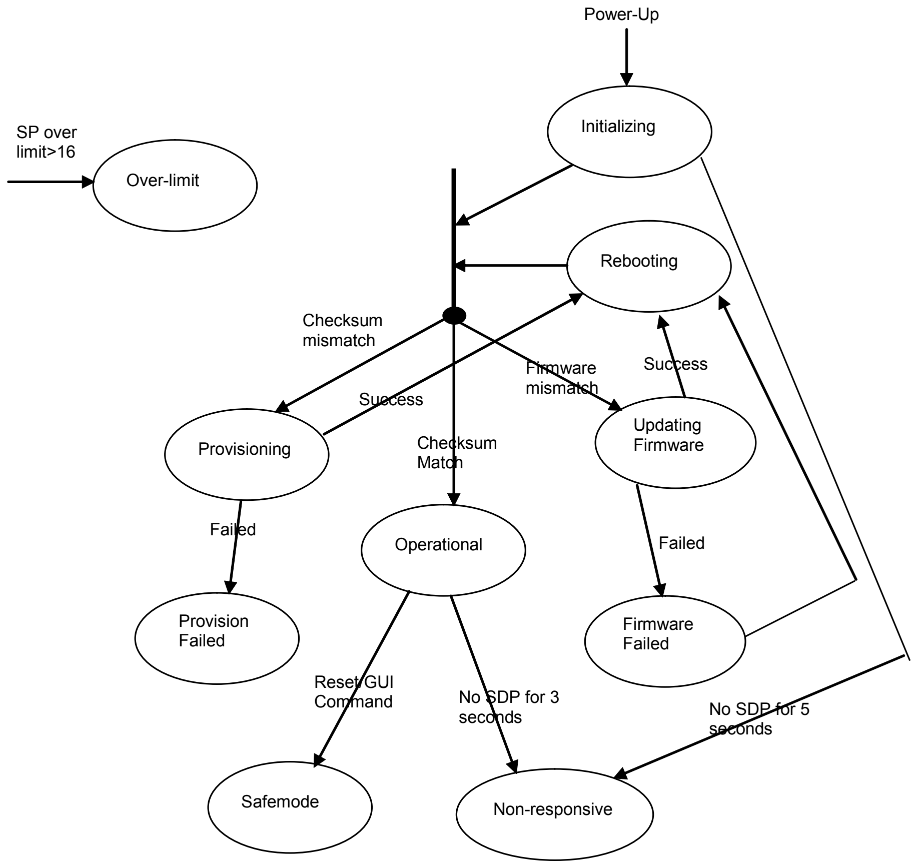
The SonicWALL Discovery Protocol (SDP) is a layer 2 protocol employed by SonicPoints and devices running SonicOS Enhanced 2.5 and higher. SDP is the foundation for the automatic provisioning of SonicPoint units via the following messages:

- **Advertisement** – SonicPoint devices without a peer will periodically and on startup announce or advertise themselves via a broadcast. The advertisement will include information that will be used by the receiving SonicOS device to ascertain the state of the SonicPoint. The SonicOS device will then report the state of all peered SonicPoints, and will take configuration actions as needed.
- **Discovery** – SonicOS devices will periodically send discovery request broadcasts to elicit responses from L2 connected SonicPoint units.
- **Configure Directive** – A unicast message from a SonicOS device to a specific SonicPoint unit to establish encryption keys for provisioning, and to set the parameters for and to engage configuration mode.
- **Configure Acknowledgement** – A unicast message from a SonicPoint to its peered SonicOS device acknowledging a Configure Directive.
- **Keepalive** – A unicast message from a SonicPoint to its peered SonicOS device used to validate the state of the SonicPoint.

If via the SDP exchange the SonicOS device ascertains that the SonicPoint requires provisioning or a configuration update (e.g. on calculating a checksum mismatch, or when a firmware update is available), the Configure directive will engage a 3DES encrypted, reliable TCP based SonicWALL Simple Provisioning Protocol (SSPP) channel. The SonicOS device will then send the update to the SonicPoint via this channel, and the SonicPoint will restart with the updated configuration. State information will be provided by the SonicPoint, and will be viewable on the SonicOS device throughout the entire discovery and provisioning process.

SonicPoint States

SonicPoint devices can function in and report the following states:


Power-Up
Initializing
SP over limit>16
Over-limit
Rebooting
Checksum mismatch
Success
Firmware mismatch
Success
Provisioning
Checksum Match
Updating Firmware
Failed
Operational
Failed
Provision Failed
Firmware Failed
Reset GUI Command
No SDP for 3 seconds
No SDP for 5 seconds
Safemode
Non-responsive

- **Initializing** – The state when a SonicPoint starts up and advertises itself via SDP prior to it entering into an operational or stand-alone mode.
- **Operational** – Once the SonicPoint has peered with a SonicOS device and has its configuration validated, it will enter into a operational state, and will be ready for clients.
- **Provisioning** – If the SonicPoint configuration requires an update, the SonicOS device will engage an SSPP channel to update the SonicPoint. During this brief process it will enter the provisioning state.
- **Safemode** – Safemode can be engaged by depressing the reset button, or from the SonicOS peer device. Placing a SonicPoint into Safemode returns its configuration to defaults, disables the radios, and disables SDP. The SonicPoint must then be rebooted to enter either a stand-alone, or some other functional state.
- **Non-Responsive** – If a SonicOS device loses communications with a previously peered SonicPoint, it will report its state as non-responsive. It will remain in this state until either communications are restored, or the SonicPoint is deleted from the SonicOS device's table.

- **Updating Firmware** – If the SonicOS device detects that it has a firmware update available for a SonicPoint, it will use SSPP to update the SonicPoint's firmware.
- **Over-Limit** – By default, up to 16 SonicPoint devices can be attached to each Wireless Zone interface on a SonicOS device. If more than 16 units are detected, the over-limit devices will report an over-limit state, and will not enter an operational mode. The number can be reduced from 16 as needed.
- **Rebooting** – After a firmware or configuration update, the SonicPoint will announce that it is about to reboot, and will then do so.
- **Firmware failed** – If a firmware update fails, the SonicPoint will report the failure, and will then reboot.
- **Provision failed** – In the unlikely event that a provision attempt from a SonicOS device fails, the SonicPoint will report the failure. So as not to enter into an endless loop, it can then be manually rebooted, manually reconfigured, or deleted and re-provisioned.
- **Stand-alone Mode (not reported)** – If a SonicPoint device cannot find or be found by a SonicOS device to peer with, it will enter a stand-alone mode of operation. This will engage the SonicPoint's internal GUI (which is otherwise disabled) and will allow it to be configured as a conventional Access Point. If at any time it is placed on the same layer 2 segment as a SonicOS device that is sending Discovery packets, it will leave stand-alone mode, and will enter into a managed mode. The stand-alone configuration will be retained.

Note: *SonicPoints can work with SonicOS Enhanced Hardware Failover. If a SonicPoint is connected to a Hardware Failover pair via a hub or switch, it will not lose connectivity when the security appliances fail over from the primary to the backup. For more information on Hardware Failover, see* ***Chapter 37, Setting Up Hardware Failover*** *and* **The SonicWALL SonicPoint Administrator's Guide**.

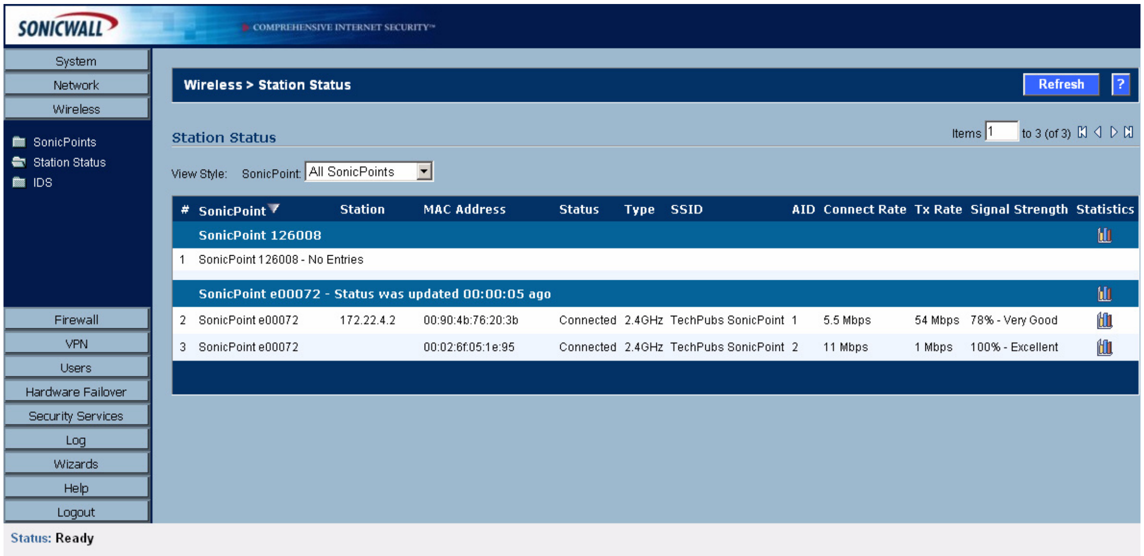
CHAPTER 21

Viewing Station Status

Wireless > Station Status

Event and Statistics Reporting

The **Wireless > Station Status** page reports on the statistics of each SonicPoint.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
SonicPoints
Station Status
IDS
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Wireless > Station Status
Refresh
?

Station Status

Items 1 to 3 (of 3)

View Style: SonicPoint: All SonicPoints

#	SonicPoint	Station	MAC Address	Status	Type	SSID	AID	Connect Rate	Tx Rate	Signal Strength	Statistics
	SonicPoint 126008										
1	SonicPoint 126008 - No Entries										
	SonicPoint e00072 - Status was updated 00:00:05 ago										
2	SonicPoint e00072	172.22.4.2	00:90:4b:76:20:3b	Connected	2.4GHz	TechPubs SonicPoint	1	5.5 Mbps	54 Mbps	78% - Very Good	
3	SonicPoint e00072		00:02:6f:05:1e:95	Connected	2.4GHz	TechPubs SonicPoint	2	11 Mbps	1 Mbps	100% - Excellent	

Status: Ready

The table lists entries for each wireless client connected to each SonicPoint. The sections of the table are divided by SonicPoint. Under each SonicPoint, is the list of all clients currently connected to it.

Click the **Refresh** button in the top right corner to refresh the list.

By default, the page displays the first 50 entries found. Click the First Page ⏮, Previous Page ◁, Next Page ▷, and Last Page ⏭ icons to navigate if you need to view more than 50 entries.

Each SonicPoint device reports for both radios, and for each station, the following information to its SonicOS peer:

- MAC Address – The client's (Station's) hardware address
- Station State – The state of the station. States can include:

  - None – No state information yet exists for the station
  - Authenticated – The station has successfully authenticated.
  - Associated – The station is associated.
  - Joined – The station has joined the ESSID.
  - Connected – The station is connected (joined, authenticated or associated).
  - Up – An Access Point state, indicating that the Access Point is up and running.
  - Down – An Access Point state, indicating that the Access Point is not running.
- Associations – Total number of Associations since power up.
- Dis-Associations – Total number of Dis-Associations.
- Re-Associations – Total number of Re-Associations.
- Authentications – Number of Authentications.
- De-Authentications – Number of De-Authentications.
- Good Frames Received – Total number of good frames received.
- Good Frames Transmitted – Total number of good frames transmitted.
- Error in Receive Frames – Total number of error frames received.
- Error in Transmit Frames – Total number of error frames transmitted.
- Discarded Frames – Total number of frames discarded. Discarded frames are generally a sign of network congestion.
- Total Bytes received – Total number of bytes received.
- Total Bytes Transmitted – Total number of bytes transmitted.
- Management Frames Received – Total number of Management frames received. Management Frames include:
  - Association request
  - Association response
  - Re-association request
  - Re-association response
  - Probe request
  - Probe response
  - Beacon frame
  - ATIM message
  - Disassociation
  - Authentication
  - De-authentication
- Management Frames Transmitted – Total number of Management frames transmitted.
- Control Frames Received – Total number of Control frames received. Control frames include:
  - RTS – Request to Send
  - CTS – Clear to Send
  - ACK – Positive Acknowledgement
- Control Frames Transmitted – Total number of Control frames transmitted.
- Data Frames Received – Total number of Data frames received.
- Data Frames Transmitted – Total number of Data frames transmitted.

CHAPTER

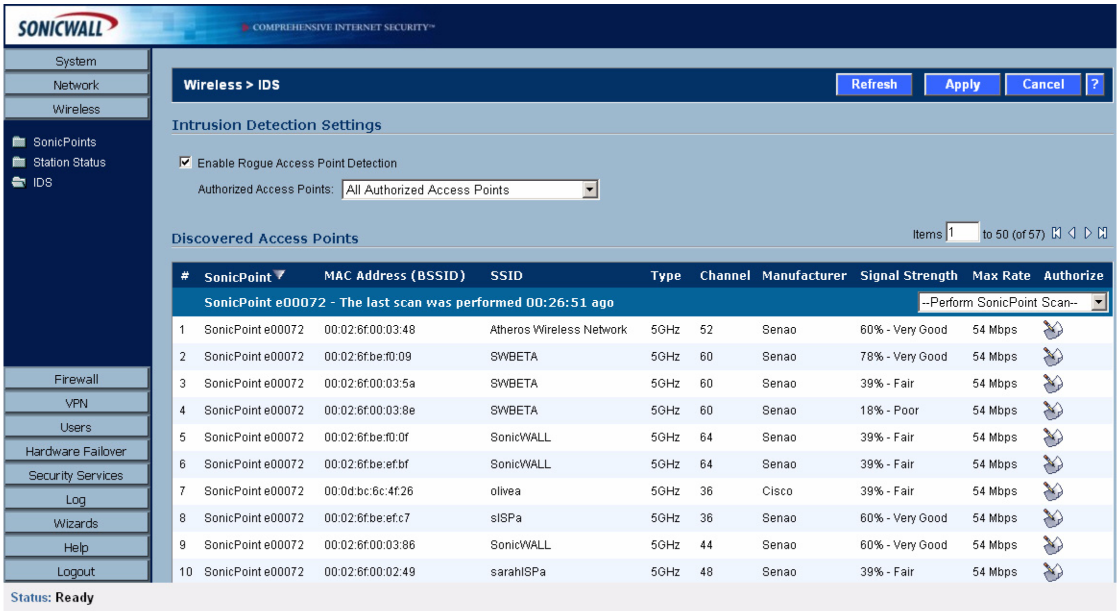
22

Using and Configuring IDS

Wireless > IDS

Detecting Wireless Access Points

You can have many wireless access points within reach of the signal of the SonicPoints on your network. The **Wireless > IDS** page reports on all access points the 5060 can find by scanning the 802.11a and 802.11g radio bands.



Intrusion Detection Settings

☑ Enable Rogue Access Point Detection

Authorized Access Points: All Authorized Access Points

Discovered Access Points

Items 1 to 50 (of 57)

SonicPoint e00072 - The last scan was performed 00:26:51 ago   --Perform SonicPoint Scan--

#	SonicPoint	MAC Address (BSSID)	SSID	Type	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
1	SonicPoint e00072	00:02:6f:00:03:48	Atheros Wireless Network	5GHz	52	Senao	60% - Very Good	54 Mbps	
2	SonicPoint e00072	00:02:6f:be:f0:09	SWBETA	5GHz	60	Senao	78% - Very Good	54 Mbps	
3	SonicPoint e00072	00:02:6f:00:03:5a	SWBETA	5GHz	60	Senao	39% - Fair	54 Mbps	
4	SonicPoint e00072	00:02:6f:00:03:8e	SWBETA	5GHz	60	Senao	18% - Poor	54 Mbps	
5	SonicPoint e00072	00:02:6f:be:f0:0f	SonicWALL	5GHz	64	Senao	39% - Fair	54 Mbps	
6	SonicPoint e00072	00:02:6f:be:ef:bf	SonicWALL	5GHz	64	Senao	39% - Fair	54 Mbps	
7	SonicPoint e00072	00:0d:bc:6c:4f:26	olivea	5GHz	36	Cisco	39% - Fair	54 Mbps	
8	SonicPoint e00072	00:02:6f:be:ef:c7	sISPa	5GHz	36	Senao	60% - Very Good	54 Mbps	
9	SonicPoint e00072	00:02:6f:00:03:86	SonicWALL	5GHz	44	Senao	60% - Very Good	54 Mbps	
10	SonicPoint e00072	00:02:6f:00:02:49	sarahISPa	5GHz	48	Senao	39% - Fair	54 Mbps	

Status: Ready

Wireless Intrusion Detection Services

Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWALL PRO 5060 by enabling it to recognize and even take countermeasures against the most common types of illicit wireless activity. IDS consists of three types of services, namely, Sequence Number Analysis, Association Flood Detection, and Rogue Access Point Detection. IDS logging and notification can be enabled under **Log > Categories** by selecting the **IDS** checkbox under **Log Categories** and **Alerts**.

Access Point IDS

When the **Radio Role** of the SonicWALL PRO 5060 is set to **Access Point** mode, all three types of WIDS services are available, but Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation). Selecting **Scan Now** momentarily changes the Radio Role to allow the PRO 5060 to perform an active scan, and may cause a brief loss of connectivity for associated wireless clients. While in **Access Point** mode, the **Scan Now** function should only be used if no clients are actively associated, or if the possibility of client interruption is acceptable.

Rogue Access Point Detection

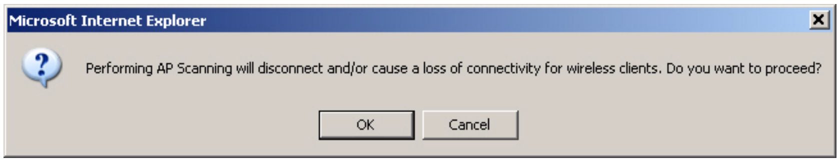
Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The PRO 5060 can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11a and 802.11g channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

Active scanning occurs when the PRO 5060 starts up, and at any time **Scan Now** is clicked on the **Wireless > IDS** page. When the PRO 5060 is operating in a Bridge Mode, the **Scan Now** feature does not cause any interruption to the bridged connectivity. When the PRO 5060 is operating in Access Point Mode, however, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.
- WiFiSec connections should automatically re-establish and resume with no noticeable interruption to the client.

▲ **Alert:** *If service disruption is a concern, it is recommended that the* ***Scan Now*** *feature not be used while the PRO 5060 is in Access Point mode until such a time that no clients are active, or the potential for disruption becomes acceptable.*



Performing AP Scanning will disconnect and/or cause a loss of connectivity for wireless clients. Do you want to proceed?

Authorizing Access Points on Your Network

Access Points detected by the PRO 5060 are regarded as rogues until they are identified to the PRO 5060 as authorized for operation. To authorize an access point, it can be manually added to the **Authorized Access Points** list by clicking **Add** and specifying its MAC address (BSSID) along with an optional comment. Alternatively, if an access point is discovered by the PRO 5060 scanning feature, it can be added to the list by clicking the **Authorize** icon.

PART

5

Firewall

:

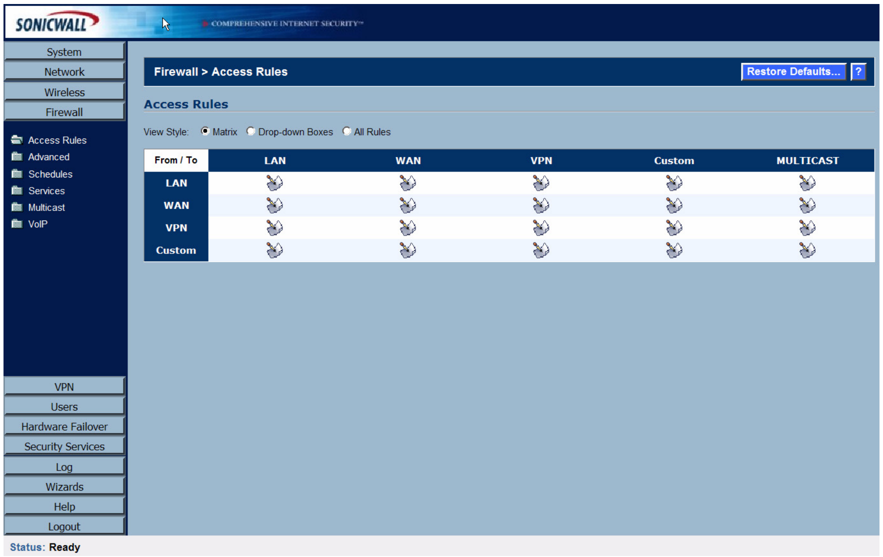
CHAPTER 23

Configuring Access Rules

Firewall > Access Rules

This chapter provides an overview on your SonicWALL security appliance stateful packet inspection default access rules and configuration examples to customize your access rules to meet your business requirements.

Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the SonicWALL security appliance.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
Access Rules
Advanced
Schedules
Services
Multicast
VoIP
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Firewall > Access Rules
Restore Defaults...
?
Access Rules

View Style: ● Matrix ○ Drop-down Boxes ○ All Rules

From / To	LAN	WAN	VPN	Custom	MULTICAST
LAN	✎	✎	✎	✎	✎
WAN	✎	✎	✎	✎	✎
VPN	✎	✎	✎	✎	✎
Custom	✎	✎	✎	✎	✎

Status: Ready

The SonicOS **Firewall > Access Rules** setting provides a sortable access rule management interface. The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.

Stateful Packet Inspection Default Access Rules Overview

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the "Default" stateful inspection packet access rule enabled in the SonicWALL security appliance:

- Allow all sessions originating from the LAN to the WAN and DMZ.
- Allow all sessions originating from the DMZ to the WAN.
- Deny all sessions originating from the WAN to the DMZ.
- Deny all sessions originating from the WAN and DMZ to the LAN.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the SonicWALL security appliance. Network access rules take precedence, and can override the SonicWALL security appliance's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the SonicWALL security appliance default setting of allowing this type of traffic.

Alert: *The ability to define network access rules is a very powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.*

Using Bandwidth Management with Access Rules Overview

Bandwidth management allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all WAN zones. Using access rules, bandwidth management can be enabled on a per-interface basis. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled WAN interface. All other packets will be queued in the default queue and will be sent in a First In and First Out (FIFO) manner (a storage method that retrieves the item stored for the longest time).

Example Scenario

If you create an access rule for outbound mail traffic (such as SMTP) and enable bandwidth management with the following parameters:

- Guaranteed bandwidth of 20 percent
- Maximum bandwidth of 40 percent
- Priority of 0 (zero)

The outbound SMTP traffic is guaranteed 20 percent of available bandwidth available to it and can get as much as 40 percent of available bandwidth. If this is the only access rule using bandwidth management, it has priority over all other access rules on the SonicWALL security appliance. Other access rules use the remaining bandwidth (minus 20 percent of bandwidth, or greater than minus 20 percent and less than minus 40 percent of bandwidth).

Note: *Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority.*

✓ **Tip:** *You must select Bandwidth Management on the **WAN > Ethernet** page. Click **Network**, then **Configure** in the **WAN** line of the **Interfaces** table, and type your available bandwidth in the **Available WAN Bandwidth** (**Kbps**) field.*

Configuration Task List

This section provides a list of the following configuration tasks:

- Displaying Access Rules with View Styles
- Configuring Access Rules for a Zone
- Adding Access Rules
- Editing an Access Rule
- Deleting an Access Rule
- Enabling and Disabling an Access Rule
- Displaying Access Rule Traffic Statistics
- Access Rule Configuration Examples

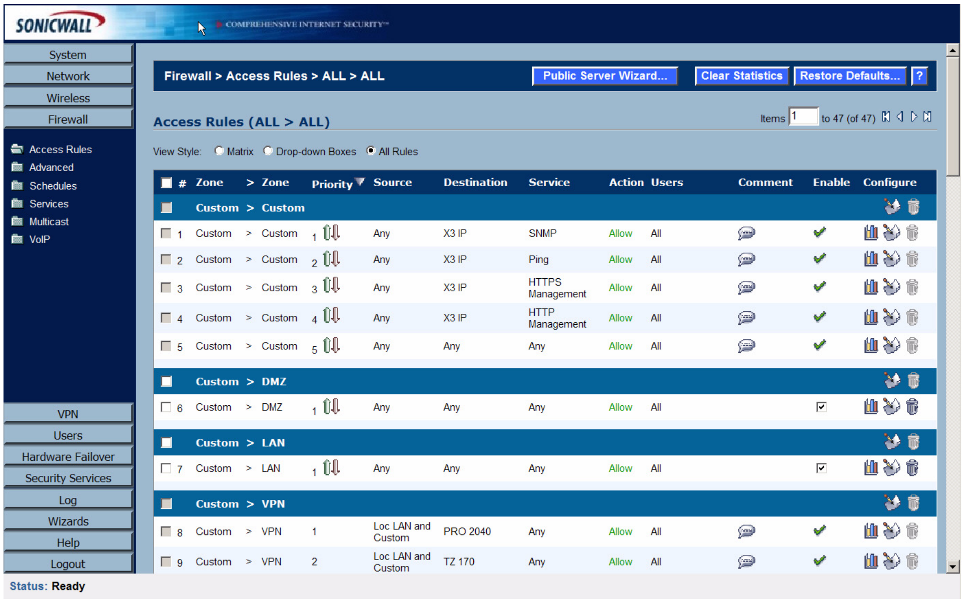
Displaying Access Rules with View Styles

Access rules can be displayed in multiple views using SonicOS Enhanced. You can select the type of view from the selections in the **View Style** section. The following **View Styles** are available:

- **Matrix** - Displays as **From/To** with **LAN**, **WAN**, **VPN**, or other interface in the **From** row, and **LAN**, **WAN**, **VPN**, or other interface in the **To** column. Select the **Notepad** icon in the table cell to view the access rules.
- **Drop-down Boxes** - Displays two pull-down menus: **From Zone** and **To Zone**. Select an interface from the **From Zone** menu and select an interface from the **To Zone** menu. Click **OK** and access rules defined for the two interfaces are displayed.
- **All Rules** - Select **All Rules** to display all access rules configured on the SonicWALL security appliance.

✓ **Tip:** *You can also view access rules by Zones. Use the Option checkboxes in the **From Zone** and **To Zone** column. Select **LAN**, **WAN**, **VPN**, **ALL** from the **From Zone** column. And then select LAN, WAN, VPN, ALL from the **To Zone** column. Click **OK** to display the access rules.*

Each view displays a table of defined network access rules. For example, selecting **All Rules** displays all the network access rules for all zones.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
Access Rules
Advanced
Schedules
Services
Multicast
VoIP
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Public Server Wizard...
Clear Statistics
Restore Defaults...
?

Firewall > Access Rules > ALL > ALL

Access Rules (ALL > ALL)

Items 1 to 47 (of 47)

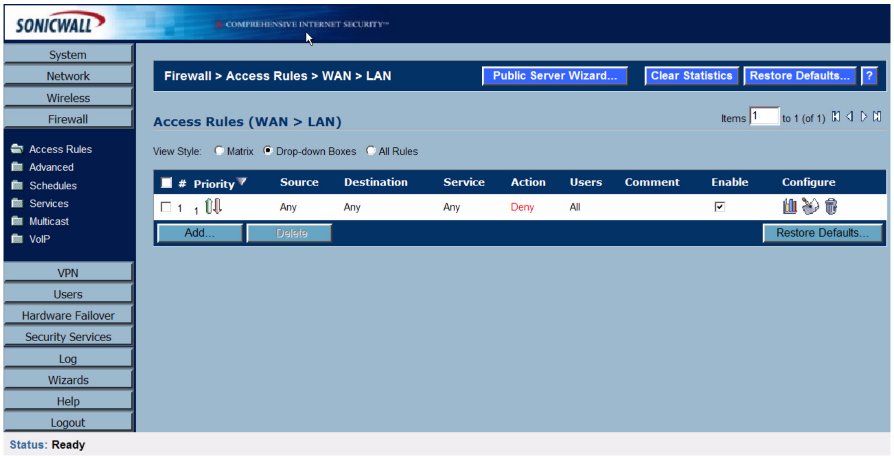
View Style: ○ Matrix ○ Drop-down Boxes ● All Rules

#	Zone	> Zone	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
	Custom	**> Custom**									
1	Custom	> Custom	1	Any	X3 IP	SNMP	Allow	All		✓	
2	Custom	> Custom	2	Any	X3 IP	Ping	Allow	All		✓	
3	Custom	> Custom	3	Any	X3 IP	HTTPS Management	Allow	All		✓	
4	Custom	> Custom	4	Any	X3 IP	HTTP Management	Allow	All		✓	
5	Custom	> Custom	5	Any	Any	Any	Allow	All		✓	
	Custom	**> DMZ**									
6	Custom	> DMZ	1	Any	Any	Any	Allow	All		☑	
	Custom	**> LAN**									
7	Custom	> LAN	1	Any	Any	Any	Allow	All		☑	
	Custom	**> VPN**									
8	Custom	> VPN	1	Loc LAN and Custom	PRO 2040	Any	Allow	All		✓	
9	Custom	> VPN	2	Loc LAN and Custom	TZ 170	Any	Allow	All		✓	

Status: Ready

Configuring Access Rules for a Zone

To display the **Access Rules** for a specific zone, select a zone from the **Matrix**, **Drop-down Boxes**, or **All Rules** view.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
Access Rules
Advanced
Schedules
Services
Multicast
VoIP
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Public Server Wizard...
Clear Statistics
Restore Defaults...
?
Add...
Delete
Restore Defaults...

Firewall > Access Rules > WAN > LAN

Access Rules (WAN > LAN)

Items 1 to 1 (of 1)

View Style: ○ Matrix ● Drop-down Boxes ○ All Rules

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Any	Any	Any	Deny	All		☑	

Status: Ready

The access rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Any** rule. The default access rule is all IP services except those listed in the **Access Rules** page. Access rules can be created to override the behavior of the **Any** rule; for example, the **Any** rule allows users on the LAN to access all Internet services, including NNTP News.

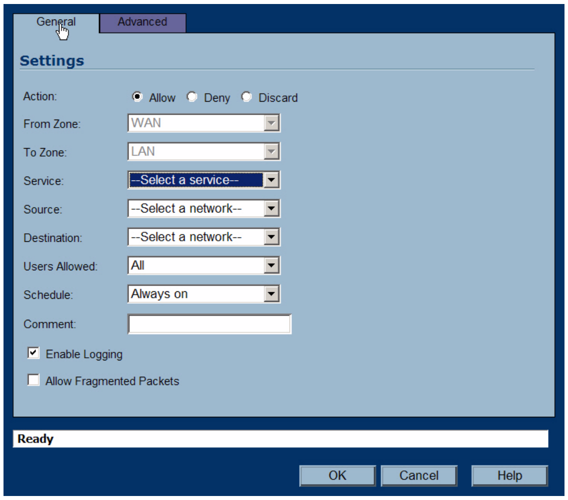
You can change the priority ranking of an access rule by clicking the **Arrows** icon in the Priority column. The Change Priority window is displayed. Enter the new priority number (1-10) in the **Priority** field, and click **OK**.

✓ **Tip:** *If the **Trashcan** or **Notepad** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.*

Adding Access Rules

To add access rules to the SonicWALL security appliance, perform the following steps:

1. Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.



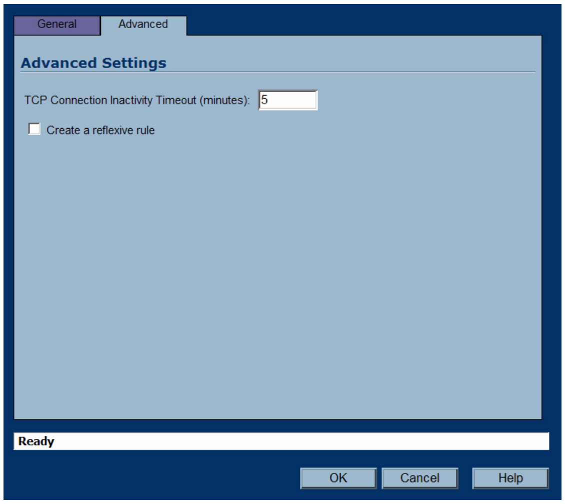
Settings

Action: ● Allow ○ Deny ○ Discard
From Zone: WAN
To Zone: LAN
Service: --Select a service--
Source: --Select a network--
Destination: --Select a network--
Users Allowed: All
Schedule: Always on
Comment:
☑ Enable Logging
☐ Allow Fragmented Packets

Ready

2. Select **Allow | Deny | Discard** from the **Action** list to permit or block IP traffic.
3. Select the service or group of services affected by the access rule from the **Service** list. The **Default** service encompasses all IP services.
   If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.
4. Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
5. If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, type the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field. To include all IP addresses, type ***** in the **Address Range Begin** field.
6. Select the destination of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
7. From the **Users Allowed** menu, add the user or user group affected by the access rule.
8. Select a schedule from the **Schedule** menu. The default schedule is **Always on**.
9. Enter any comments to help identify the access rule in the **Comments** field.

10. Click on the **Advanced** tab.



Advanced Settings

TCP Connection Inactivity Timeout (minutes): 5

☐ Create a reflexive rule

Ready

11. Do not select the **Allow Fragmented Packets** check box. Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. Because hackers exploit IP fragmentation in Denial of Service (DoS) attacks, the SonicWALL security appliance blocks fragmented packets by default. You can override the default configuration to allow fragmented packets over PPTP or IPSec.
12. If you would like for the access rule to timeout after a period of inactivity, set the amount of time, in minutes, in the **Inactivity Timeout (minutes)** field. The default value is 5 minutes.
13. Click the **Bandwidth** tab. Select **Enable Outbound Bandwidth Management** (**'allow' rules only),** and enter the **Guaranteed Bandwidth** in Kbps.
14. Enter the maximum amount of bandwidth available to the access rule at any time in the **Maximum Bandwidth** field.

✓ **Tip:** *Access rules using bandwidth management take priority over access rules without bandwidth management.*

15. Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** list.
16. Click **OK**.

✓ **Tip:** *Although custom access rules can be created that allow inbound IP traffic, the SonicWALL security appliance does not disable protection from DoS attacks, such as the SYN Flood and Ping of Death attacks.*

Editing an Access Rule

To display the **Edit Rule** window (includes the same settings as the **Add Rule** window), click the **Notepad** icon.

Deleting an Access Rule

To delete the individual access rule, click on the **Trashcan** icon. To delete all the checkbox selected access rules, click the **Delete** button.

Enabling and Disabling an Access Rule

To enable or disable an access rule, click the **Enable** checkbox.

Restoring Access Rules to Default Zone Settings

To remove all end-user configured access rules for a zone, click the **Default** button. This will restore the access rules for the selected zone to the default access rules initially setup on the SonicWALL security appliance.

Displaying Access Rule Traffic Statistics

Move your mouse pointer over the **Graph** icon to display the following access rule receive (Rx) and transmit (Tx) traffic statistics:

- Rx Bytes
- Rx Packets
- Tx Bytes
- Tx Packets

Access Rule Configuration Examples

This section provides configuration examples on adding network access rules:

- Enabling Ping
- Blocking LAN Access for Specific Services
- Enabling Bandwidth Management on an Access Rule

Enabling Ping

This sections provides a configuration example for an access rule to allow devices on the DMZ to send ping requests and receive ping responses from devices on the LAN. By default your SonicWALL security appliance does not allow traffic initiated from the DMZ to reach the LAN. Once you have placed one of your interfaces into the DMZ zone, then from the **Firewall** > **Access Rules** window, perform the following steps to configure an access rule that allow devices in the DMZ to send ping requests and receive ping esponses from devices in the LAN.

1. From the **DMZ** > **LAN** page, click the **Edit** icon.
2. Click **Add** to launch the **Add Rule** window.
3. Select the **Allow** radio button.
4. From the **Service** menu, select **Ping**.
5. From the **Source** menu, select **DMZ Subnets**.
6. From the **Destination** menu, select **LAN Subnets**.
7. Click **OK**.

Blocking LAN Access for Specific Services

This section provides a configuration example for an access rule blocking LAN access to NNTP servers on the Internet during business hours.

Perform the following steps to configure an access rule blocking LAN access to NNTP servers based on a schedule:

1. Click **Add** to launch the **Add** window.
2. Select **Deny** from the **Action** settings.
3. Select **NNTP** from the **Service** menu. If the service is not listed in the list, you must to add it in the **Add Service** window.
4. Select **Any** from the **Source** menu.
5. Select **X1** from the **Destination** menu.
6. Select the schedule from the **Schedule** menu.
7. Enter any comments in the **Comment** field.
8. Click **OK**.

Enabling Bandwidth Management on an Access Rule

Bandwidth management can be applied on both ingress and egress traffic using access rules. Access rules displaying the Funnel icon are configured for bandwidth management.

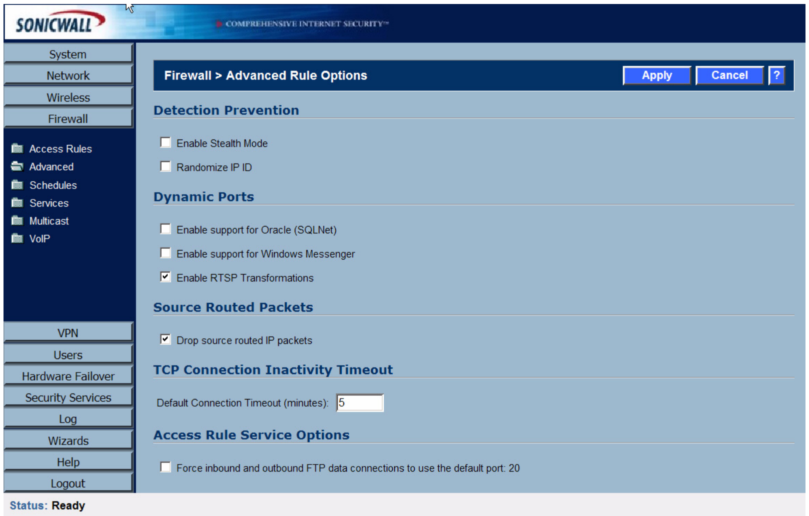
✓ **Tip**: *Do not configure bandwidth management on multiple interfaces on a zone, where the configured guaranteed bandwidth for the zone is greater than the available bandwidth for the bound interface.*

CHAPTER 24

Configuring Advanced Access Rule Settings

Firewall > Advanced

To configure advanced access rule options, select **Firewall > Advanced** under Firewall. The **Advanced Rule Options** page is displayed..


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
Access Rules
Advanced
Schedules
Services
Multicast
VoIP
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?

Firewall > Advanced Rule Options

Detection Prevention

☐ Enable Stealth Mode
☐ Randomize IP ID

Dynamic Ports

☐ Enable support for Oracle (SQLNet)
☐ Enable support for Windows Messenger
☑ Enable RTSP Transformations

Source Routed Packets

☑ Drop source routed IP packets

TCP Connection Inactivity Timeout

Default Connection Timeout (minutes): 5

Access Rule Service Options

☐ Force inbound and outbound FTP data connections to use the default port: 20

Status: Ready

The **Advanced Rule Options** includes the following firewall configuration option groups:

- **Detection Prevention**
- **Dynamic Ports**
- **Source Routed Packets**
- **TCP Connection Inactivity Timeout**
- **Access Rule Service Options**

Detection Prevention

- **Enable Stealth Mode** - By default, the security appliance responds to incoming connection requests as either “blocked” or “open.” If you enable Stealth Mode, your security appliance does not respond to *blocked inbound connection requests*. Stealth Mode makes your security appliance essentially invisible to hackers.
- **Randomize IP ID** - Select Randomize IP ID to prevent hackers using various detection tools from detecting the presence of a security appliance. IP packets are given random IP IDs, which makes it more difficult for hackers to “fingerprint” the security appliance.

Dynamic Ports

- **Enable support for Oracle (SQLNet)** - Select if you have Oracle applications on your network.
- **Enable support for Windows Messenger** - Select this option to support special SIP messaging used in Windows Messenger on the Windows XP.
- **Enable RTSP Transformations** - Select this option to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.

Source Routed Packets

Drop Source Routed Packets is selected by default. Clear the check box if you are testing traffic between two specific hosts and you are using source routing.

TCP Connection Inactivity Timeout

If a connection to a remote server remains idle for more than five minutes, the security appliance closes the connection. Without this timeout, Internet connections could stay open indefinitely, creating potential security holes. You can increase the **Inactivity Timeout** if applications, such as Telnet and FTP, are frequently disconnected.

Access Rule Service Options

Force inbound and outbound FTP data connections to use default port 20 - The default configuration allows FTP connections from port 20 but remaps outbound traffic to a port such as 1024. If the check box is selected, any FTP data connection through the security appliance must come from port 20 or the connection is dropped. The event is then logged as a log event on the security appliance.

CHAPTER

25

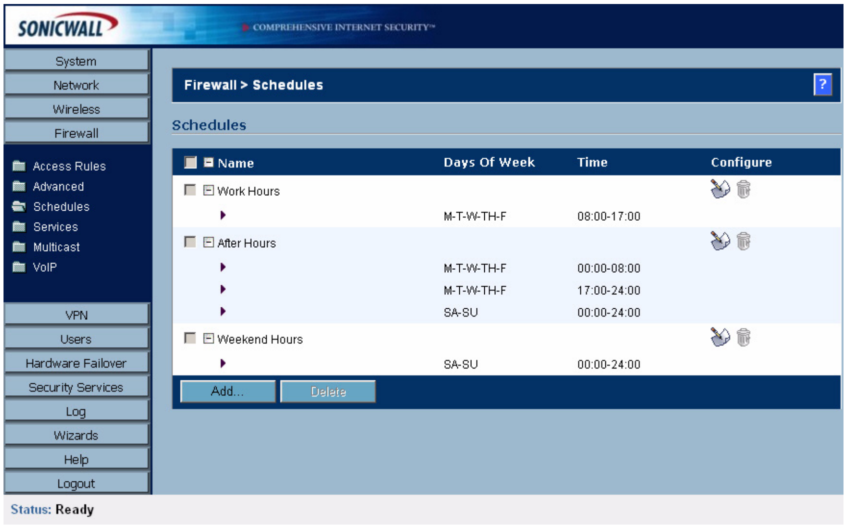
Setting Access Rule Schedules

Firewall > Schedules

The **Firewall>Schedules** page allows you to create and manage access rule enforcement schedules. The **Schedules** table displays all your predefined and custom schedules.

Schedules

The SonicWALL has the flexibility to create and add schedules for Access Rules or Access Rule Groups.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
Access Rules
Advanced
Schedules
Services
Multicast
VoIP
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Firewall > Schedules
?
Schedules
Add...
Delete
Status: Ready

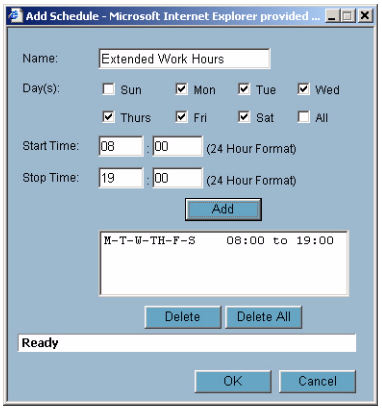
Name	Days Of Week	Time	Configure
Work Hours			
	M-T-W-TH-F	08:00-17:00	
After Hours			
	M-T-W-TH-F	00:00-08:00	
	M-T-W-TH-F	17:00-24:00	
	SA-SU	00:00-24:00	
Weekend Hours			
	SA-SU	00:00-24:00	

In the **Schedules** table, there are three default schedules: **Work Hours**, **After Hours**, and **Weekend Hours**. You can modify these schedule by clicking on the Edit icon in the **Configure** column.

A schedule can include multiple day and time increments for rule enforcement with a single schedule. If a schedule includes multiple day and time entries, a **+** (expand) button appears next to the schedule name. Clicking the + button expands the schedule to display all the day and time entries for the schedule.

Adding a Schedule

To create schedules, click **Add**. The **Add Schedule** window is displayed.



Name: Extended Work Hours

Day(s): ☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thurs ☑ Fri ☑ Sat ☐ All

Start Time: 08 : 00 (24 Hour Format)

Stop Time: 19 : 00 (24 Hour Format)

```
M-T-W-TH-F-S     08:00 to 19:00
```

Ready

1 Enter a name for the schedule in the **Name** field.
2 Select the days of the week to apply to the schedule or select **All**.
3 Enter the time of day for the schedule to begin in the **Start** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
4 Enter the time of day for the schedule to stop in the **Stop** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
5 Click **Add**.
6 Click **OK** to add the schedule to the **Schedules** table.
7 To delete existing days and times, select the schedule and click **Delete**. Or, to delete all existing schedules, click **Delete All**.

Deleting Schedules

To delete individual Schedules, select the checkbox next to the Schedule, the **Delete** button becomes enabled. Click **Delete**. To delete all Schedules, select the checkbox next to **Name** to select all Schedules. Click **Delete**.

CHAPTER

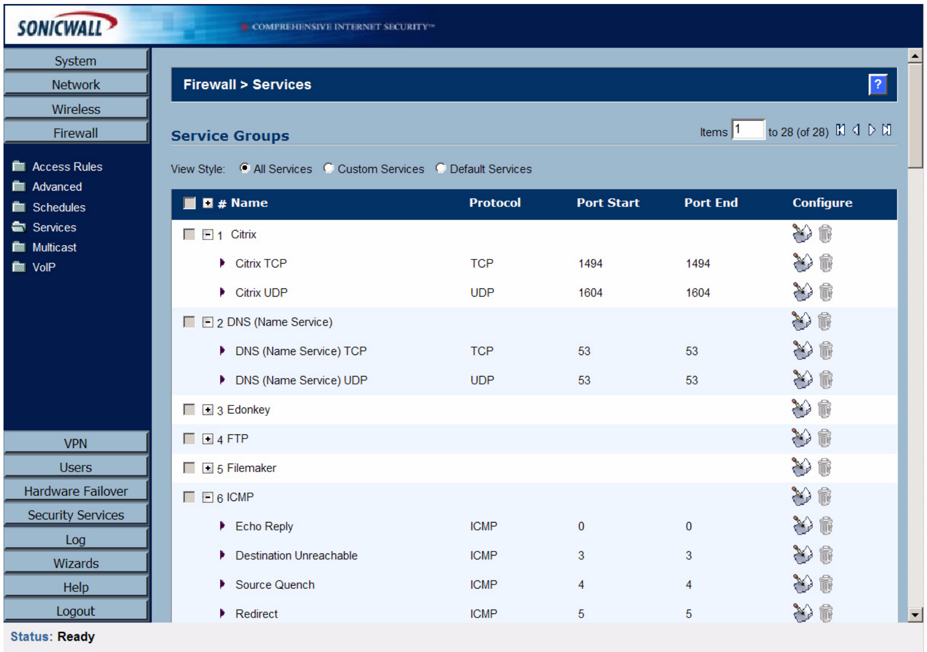
26

Configuring Firewall Services

Firewall > Services

SonicOS Enhanced supports an expanded IP protocol support to allow users to create services and access rules based on these protocols. See “Supported Protocols” on page 146 for a complete listing of support IP protocols.

Services are used by the SonicWALL security appliance to configure network access rules for allowing or denying traffic to the network. The SonicWALL security appliance includes **Default Services**. Default Services are predefined services that are not editable. And you can also create **Custom Services** to configure firewall services to meet your specific business requirements.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
Access Rules
Advanced
Schedules
Services
Multicast
VoIP
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Firewall > Services
?
Service Groups
Items 1 to 28 (of 28)
View Style: ● All Services ○ Custom Services ○ Default Services
Status: Ready

# Name	Protocol	Port Start	Port End	Configure
1 Citrix				
Citrix TCP	TCP	1494	1494	
Citrix UDP	UDP	1604	1604	
2 DNS (Name Service)				
DNS (Name Service) TCP	TCP	53	53	
DNS (Name Service) UDP	UDP	53	53	
3 Edonkey				
4 FTP				
5 Filemaker				
6 ICMP				
Echo Reply	ICMP	0	0	
Destination Unreachable	ICMP	3	3	
Source Quench	ICMP	4	4	
Redirect	ICMP	5	5	

Selecting **All Services** from **View Style** displays both **Custom Services** and **Default Services**.

Default Services Overview

The **Default Services** view displays the SonicWALL security appliance default services in the **Services** table and **Service Groups** table. The Service Groups table displays clusters of multiple default services as a single service object. You cannot delete or edit these predefined services. The **Services** table displays the following attributes of the services:

- **Name**—the name of the service
- **Protocol**—the protocol of the service
- **Port Start**—the starting port number for the service
- **Port End**—the ending port number for the service
- **Configure**—Displays the unavailable Notepad and Trashcan icon (default services cannot be edited or deleted, you will need to add a new service for the Notepad and Trashcan icons to become available).

Services that apply to common applications are grouped as **Default Service Groups**. These groups cannot be changed or deleted. Clicking on the + to the left of the Default Service Groups entry, displays all the individual Default Services included in the group. For example, the **DNS** (**Name Service**) entry has two services labelled **DNS** (**Name Service**) **TCP** for port 53 and **DNS** (**Name Service**) **UDP** for port 53. These multiple entries with the same name are grouped together, and are treated as a single service. Default Services Groups cannot be edited or deleted.

Custom Services Configuration Task List

The following list provides configuration tasks for Custom Services:

- Adding Custom Services
- Editing Custom Services
- Deleting Custom Services
- Editing Custom Services Groups
- Deleting Custom Services Groups

Supported Protocols

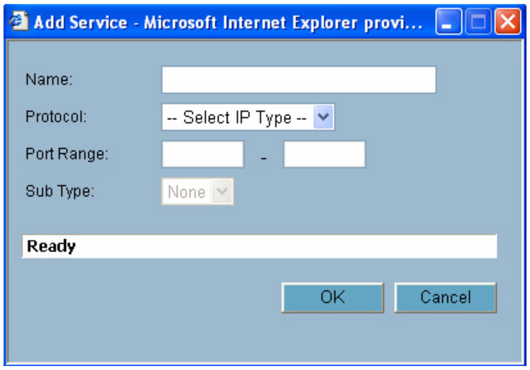
The following IP protocols are available for custom services:

- **ICMP** (**1**)—(Internet Control Message Protocol) A TCP/IP protocol used to send error and control messages.
- **IGMP** (**2**)—(Internet Group Management Protocol) The protocol that governs the management of multicast groups in a TCP/IP network.
- **TCP** (**6**)—(Transmission Control Protocol) The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.
- **UDP** (**17**)—(User Datagram Protocol) A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
- **GRE** (**47**)—(Generic Routing Encapsulation) A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP internetwork.
- **ESP** (**50**)—(Encapsulated Security Payload) A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPSec.
- **AH** (**51**)—(Authentication Header) A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).

- **EIGRP** (**88**)—(Enhanced Interior Gateway Routing Protocol) Advanced version of IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
- **OSPF** (**89**)—(Open Shortest Path First) A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.
- **PIMSM** (**103**)—(Protocol Independent Multicast Sparse Mode) One of two PIM operational modes (dense and sparse). PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs.
- **L2TP** (**115**)—(Layer 2 Tunneling Protocol) A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPSec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN.

Adding Custom Services

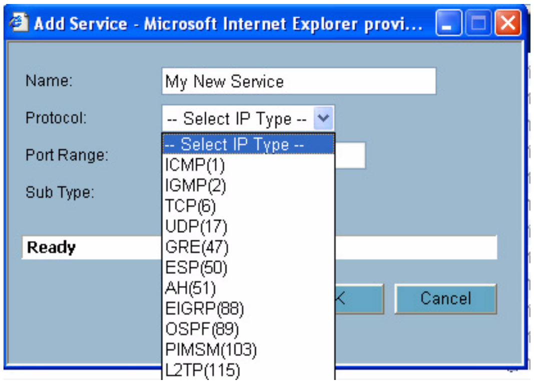
All custom services you create are listed in the **Custom Services** table. You can group custom services by creating a **Custom Services Group** for easy policy enforcement. If a protocol is not listed in the **Default Services** table, you can add it to the Custom Services table by clicking **Add**.


Add Service - Microsoft Internet Explorer provi...
Name:
Protocol:
-- Select IP Type --
Port Range:
Sub Type:
None
OK
Cancel

Ready

1 Enter the name of the service in the **Name** field.

2 Select the type of IP protocol from the **Protocol** pull-down menu.


Add Service - Microsoft Internet Explorer provi...
Protocol:
-- Select IP Type --
Port Range:
Sub Type:
-- Select IP Type --
ICMP(1)
IGMP(2)
TCP(6)
UDP(17)
GRE(47)
ESP(50)
AH(51)
EIGRP(88)
OSPF(89)
PIMSM(103)
L2TP(115)
Cancel

Name: My New Service

Ready

Enter the Port Range or IP protocol Sub Type depending on your IP protocol selection:

- For TCP and UDP protocols, specify the Port Range. You will not need to specify a Sub Type.

- For ICMP, IGMP, OSPF and PIMSM protocols, select from the Sub Type pull-down menu for sub types.
- For the remaining protocols, you will not need to specify a Port Range or Sub Type.

3. Click **OK**. The service appears in the **Custom Services** table.

Click the **Enable Logging** checkbox to disable or enable the logging of the service activities.

Editing Custom Services

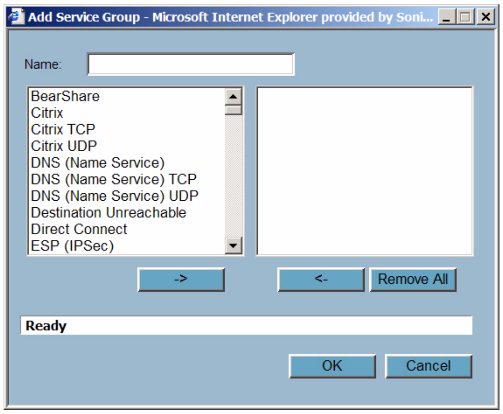
Click the **Notepad** icon under **Configure** to edit the service in the **Edit Service** window, which includes the same configuration settings as the **Add Service** window.

Deleting Custom Services

Click the **Trashcan** icon to delete an individual custom service. You can delete all custom services by clicking the **Delete** button.

Adding a Custom Services Group

You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a Custom Service Group. To create a **Custom Services Group**, click **Add Group**.


Add Service Group - Microsoft Internet Explorer provided by Soni...
Name:
BearShare
Citrix
Citrix TCP
Citrix UDP
DNS (Name Service)
DNS (Name Service) TCP
DNS (Name Service) UDP
Destination Unreachable
Direct Connect
ESP (IPSec)
->
<-
Remove All
Ready
OK
Cancel

1. Enter a name for the custom group in the name field.
2. Select individual services from the list in the left column. You can also select multiple services by pressing the Ctrl key and clicking on the services.
3. Click **- >** to add the services to the group.
4. To remove services from the group, select individual services from the list in right column. You can also select multiple services by pressing the **Ctrl** key on your keyboard and clicking on the services.
5. Click **< -** to remove the services.
6. When you are finished, click **OK** to add the group to **Custom Services Groups**.

Clicking**+** on the left of a Custom Service Group name, expands the display to show all the individual Custom Services, Default Services, and Custom Services Groups included in the Custom Service Group entry.

Editing Custom Services Groups

Click the **Notepad** icon under **Configure** to edit the custom service group in the **Edit Service Group** window, which includes the same configuration settings as the **Add Service Group** window.

Deleting Custom Services Groups

Click the **Trashcan** icon to delete the individual custom service group entry. You can delete all custom service groups by clicking the Delete button.

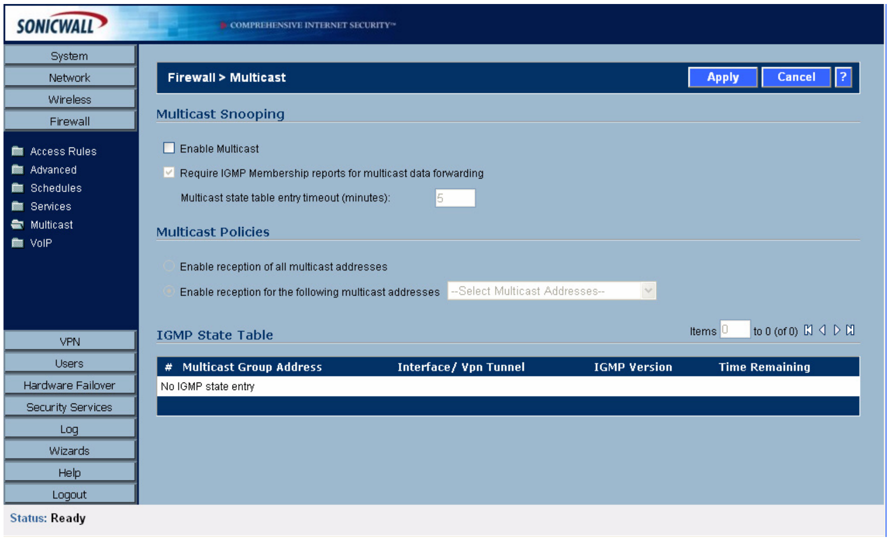
CHAPTER 27

Configuring Multicast Settings

Firewall > Multicast

Multicasting, also called IP multicasting, is a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic - multimedia presentations and videoconferencing. For example, a single host transmitting an audio or video stream and ten hosts that want to receive this stream. In mutlicasting, the sending host transmits a single IP packet with a specific multicast address, and the 10 hosts simply need to be configured to listen for packets targeted to that address to receive the transmission. Multicasting is a point-to-multipoint IP communication mechanism that operates in a connectionless mode - hosts receive multicast transmissions by "tuning in" to them, a process similar to tuning in to a radio.

The **Firewall > Multicast** page allows you to manage multicast traffic on the SonicWALL security appliance.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
Access Rules
Advanced
Schedules
Services
Multicast
VoIP
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Firewall > Multicast
Apply
Cancel
?

Multicast Snooping

☐ Enable Multicast

☑ Require IGMP Membership reports for multicast data forwarding

Multicast state table entry timeout (minutes): 5

Multicast Policies

○ Enable reception of all multicast addresses

● Enable reception for the following multicast addresses --Select Multicast Addresses--

IGMP State Table

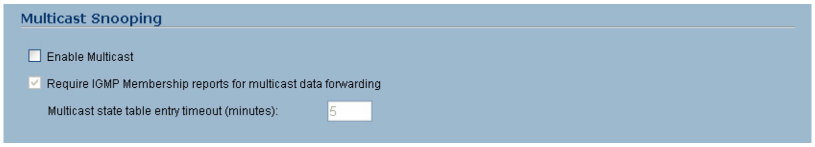
Items 0 to 0 (of 0)

#	Multicast Group Address	Interface/ Vpn Tunnel	IGMP Version	Time Remaining
No IGMP state entry				

Status: Ready

Multicast Snooping

This section provides configuration tasks for Multicast Snooping.



Multicast Snooping

☐ Enable Multicast

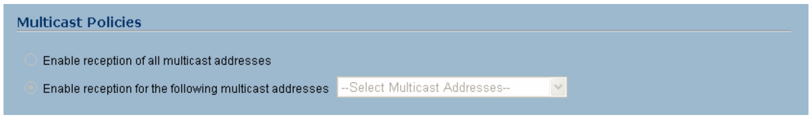
☑ Require IGMP Membership reports for multicast data forwarding

Multicast state table entry timeout (minutes): 5

- **Enable Multicast** - This checkbox is disabled by default. Select this checkbox to support multicast traffic.
- **Require IGMP Membership reports for multicast data forwarding** - This checkbox is enabled by default. Select this checkbox to improve performance by regulating multicast data to be forwarded to only interfaces belonging to an enabled multicast group address.
- **Multicast state table entry timeout (minutes)** - This field has a default of 5. The value range for this field is 5 to 60 (minutes). Update the default timer value of 5 in the following conditions:
  - You suspect membership queries or reports are being lost on the network.
  - You want to reduce the IGMP traffic on the network and currently have a large number of multicast groups or clients. This is a condition where you do not have a router to route traffic.
  - You want to synchronize the timing with an IGMP router.

Multicast Policies

This section provides configuration tasks for Multicast Policies.



Multicast Policies

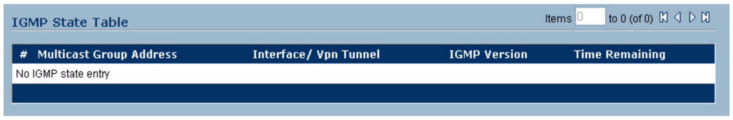
○ Enable reception of all multicast addresses

○ Enable reception for the following multicast addresses --Select Multicast Addresses--

- **Enable reception of all multicast addresses** - This radio button is not enabled by default. Select this radio button to receive all (class D) multicast addresses. Receiving all multicast addresses may cause your network to experience performance degradation.
- **Enable reception for the following multicast addresses** - This radio button is enabled by default. In the pull-down menu, select **Create a new multicast object** or **Create new multicast group**.

IGMP State Table

This section provides descriptions of the fields in the **IGMP State** table.



IGMP State Table

Items 0 to 0 (of 0)

# Multicast Group Address	Interface/ Vpn Tunnel	IGMP Version	Time Remaining
No IGMP state entry			

- **Multicast Group Address**—Provides the multicast group address the interface is joined to.
- **Interface / VPN Tunnel**—Provides the interface (such as X0) or the VPN policy.
- **IGMP Version**—Provides the IGMP version (such as V2 or V3).
- **Time Remaining**—Provides the amount of time left before the IGMP entry will be flushed. This is calculated by subtracting the "**Multicast state table entry timeout** (**minutes**)" value, which has the default value of 5 minutes, and the elapsed time since the multicast address was added.

Configuration Example

Perform the following steps to enable multicast support on LAN-dedicated interfaces.

1. Enable multicast support on your SonicWALL security appliance. In the **Firewall** > **Multicast** setting, click on the **Enable Multicast** checkbox. And in the Multicast Policy section, select the **Enable the reception of all multicast addresses**.
2. Enable multicast support on LAN interfaces. In the **Network** > **Interfaces** setting, click on the '**Configure**' icon for the X0 LAN interface. In the **Edit Interface - X0** page, click on the **Enable Multicast Support** checkbox.

Perform the following steps to enable multicast support for address objects over a VPN tunnel.

1. Enable multicast support on your SonicWALL security appliance. In the **Firewall** > **Multicast** setting, click on the **Enable Multicast** checkbox. And in the Multicast Policy section, select the **Enable the reception for the following multicast addresses** and select from the pull-down menu, **Create new multicast address object...**.
2. Create a multicast address object. In the Add Address Object window, enter the following information for your address object:
   - **Name**
   - **Zone Assignment**: <LAN, WAN, DMZ, VPN, Multicast, WLAN, Custom GroupVPN>
   - **Type**: <Host, Range, Network, MAC>
     - If you select **Host**, you will need to enter an **IP address**.
     - If you select **Range**, you will need to enter a **Starting IP Address** and an **Ending IP Address**.
     - If you select **Network**, you will need to enter a description of the **Network** and a **Netmask**.
     - If you select **MAC**, you will need to enter a **MAC Address**.
3. Enable multicast support on the VPN policy for your GroupVPN. In the **VPN** > **Settings** firmware setting, click on the "**Configure**' icon to edit your GroupVPN's VPN policy.
4. In the **VPN Policy** window, select the **Advanced** tab. At the **Advanced** tab, select the **Enable Multicast** checkbox.

CHAPTER

28

Configuring VoIP Support

This chapter provides overview information and configuration tasks on enabling Voice over IP (VoIP) protocols. VoIP is a term used in IP telephony for a set of facilities for managing the delivery of voice information using IP. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by traditional telephone service.

Firewall > VoIP

The SonicWALL security appliance supports the most widely used VoIP standard protocols and the most commonly used VoIP vendors and systems on the market. Providing full VoIP support on the SonicWALL security appliance enables organizations with increasingly decentralized workforces to access corporate voice services from remote sites. VoIP systems consist of multiple clients (such as IP phones or soft phones) and VoIP servers residing at different parts of the network.

VoIP Protocols

This section provides a concept overview on H.323 and SIP protocols. Refer to the “Configuring the VoIP Settings” section for configuration tasks for H.323 and SIP networks.

H.323

H.323 is a comprehensive suite of protocols for voice, video, and data communications between computers, terminals, network devices, and network services. H.323 is designed to enable users to make point-to-point multimedia phone calls over connectionless packet-switching networks such as private IP networks and the Internet.

H.323 is widely supported by manufacturers of video conferencing equipment, VoIP equipment and Internet telephony software and devices.

An H.323 network consists of four different types of entities:

- **Terminals** - Client end points for multimedia communications. An example would be an H.323 enabled Internet phone or PC
- **Gateways** - Connectivity between H.323 networks and other communications services, such as the circuit-switched Packet Switched Telephone Network (PSTN)

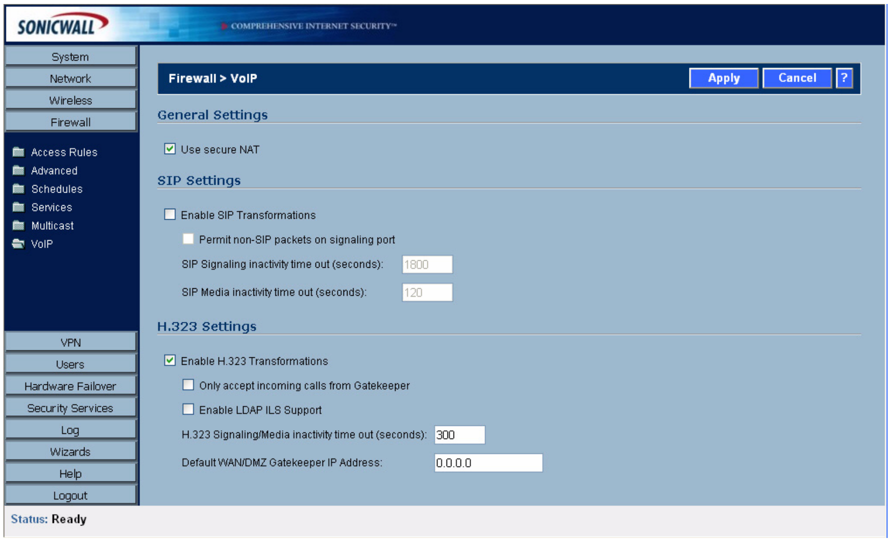
- **Gatekeepers** - Services for call setup and tear down, and registering H.323 terminals for communications
- **Multipoint control units (MCUs)** - Three-way and higher multipoint communications between terminals

SIP

Session Initiation Protocol (SIP) is a signaling protocol used in VoIP. Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration. SIP was also designed to avoid the heavy overhead of H.323.

Configuring the VoIP Settings

The SonicWALL security appliance allows VoIP phone and applications to be deployed behind the firewall. The **Firewall > VoIP** page includes the settings for supporting VoIP traffic on the SonicWALL security appliance.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
Access Rules
Advanced
Schedules
Services
Multicast
VoIP
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Firewall > VoIP
Apply
Cancel
?
Status: Ready

General Settings

☑ Use secure NAT

SIP Settings

☐ Enable SIP Transformations

☐ Permit non-SIP packets on signaling port

SIP Signaling inactivity time out (seconds): 1800

SIP Media inactivity time out (seconds): 120

H.323 Settings

☑ Enable H.323 Transformations

☐ Only accept incoming calls from Gatekeeper

☐ Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds): 300

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

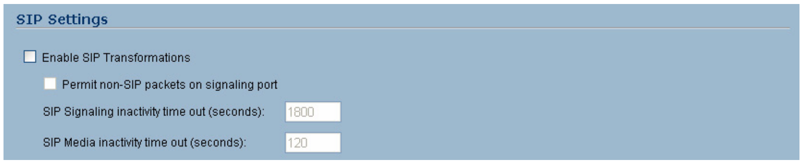
General Settings

This section provides a configuration task for Consistent NAT.

Consistent NAT - This checkbox is disabled by default. Consistent NAT may need to be enabled for applications such as Apple iChat. Check this checkbox to maintain non-rotating NAT mappings on your firewall.

SIP Settings

This section provides configuration tasks for SIP Settings.



SIP Settings

☐ Enable SIP Transformations

☐ Permit non-SIP packets on signaling port

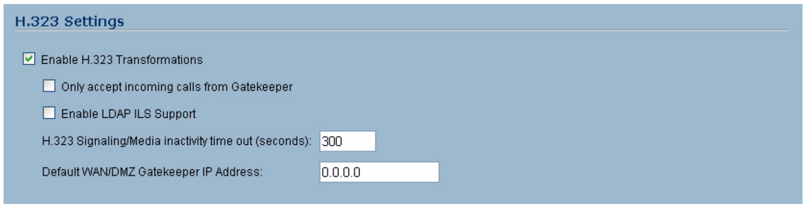
SIP Signaling inactivity time out (seconds): 1800

SIP Media inactivity time out (seconds): 120

- **Enable SIP Transformations -** This setting transforms SIP messages between LAN (trusted) and WAN/DMZ (untrusted). You need to check this setting when you want the SonicWALL to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the SonicWALL and SIP clients are on the LAN side, the SIP clients by default embed/use their private IP address in the SIP/Session Definition Protocol (SDP) messages that are sent to the SIP proxy, hence these messages are not changed and the SIP proxy does not know how to get back to the client behind the SonicWALL. Selecting **Enable SIP Transformations** enables the SonicWALL to go through each SIP message and change the private IP address and assigned port. **Enable SIP Transformation** also controls and opens up the RTP/RTCP ports that need to be opened for the SIP session calls to happen. NAT translates Layer 3 addresses but not the Layer 7 SIP/SDP addresses, which is why you need to select Enable SIP Transformations to transform the SIP messages. It's recommended that you turn on **Enable SIP Transformations** unless there is another NAT traversal solution that requires this feature to be turned off. SIP Transformations works in bi-directional mode and it transforms messages going from LAN to WAN and vice versa.
- **Permit non-SIP packets on signaling port** - This checkbox is disabled by default. Select this checkbox for enabling applications such as Apple iChat. Enabling this checkbox may open your network to malicious attacks caused by malformed or invalid SIP traffic.
- **SIP Signaling inactivity time out (seconds)** - This field has a default value of 1200 seconds (20 minutes).
- **SIP Media inactivity time out (seconds)** - This field has a default value of 120 seconds (2 minutes).

H.323 Settings

This section provides configuration tasks for H.323 Settings.



H.323 Settings

☑ Enable H.323 Transformations

☐ Only accept incoming calls from Gatekeeper

☐ Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds): 300

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

- **Enable H.323 Transformation** - Select this option to allow stateful H.323 protocol-aware packet content inspection and modification by the SonicWALL. The SonicWALL performs any dynamic IP address and transport port mapping within the H.323 packets, which is necessary for communication between H.323 parties in trusted and untrusted networks/zones. Clear the **Enable H.323 Transformation** to bypass the H.323 specific processing performed by the SonicWALL.
- **Only accept incoming calls from Gatekeeper** - Select this checkbox to ensure all incoming calls go through the Gatekeeper for authentication. The Gatekeeper will refuse calls that fail authentication.
- **Enable LDAP ILS Support** - LDAP stands for Lightweight Directory Access Protocol, a standard protocol for accessing information in a directory. ILS stands for Internet Locator Service, a LDAP service that enables Microsoft NetMeeting users to locate and connect to users for conferencing and collaboration over the Internet.

- **H.323 Signaling/Media inactivity time out (seconds)** - This field has a default value of 300 seconds (5 minutes). This is a similar setting to the “TCP connection inactivity timeout.”
- **Default WAN/DMZ Gatekeeper IP Address** - This field has a default value of 0.0.0.0. Enter the default H.323 Gatekeeper IP address in this field to allow LAN-based H.323 devices ti “discover” the gatekeeper using the multicast address 224.0.1.41. If you do not enter an IP address, multicast discovery messages from LAN-based H.323 devices will go through the configured multicast handling.

PART

6

VPN

:

CHAPTER

29

Configuring VPN Policies

VPN > Settings

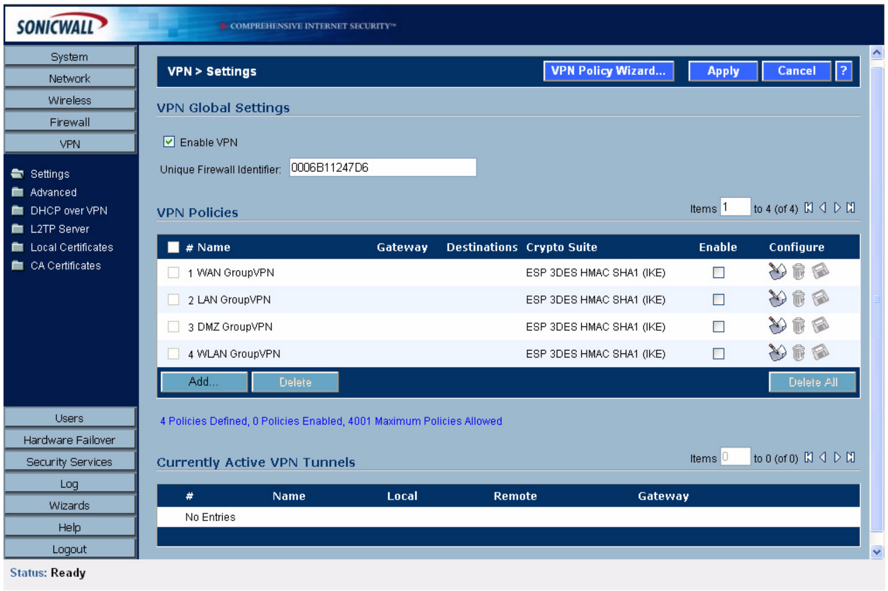
SonicWALL VPN, based on the industry-standard IPSec VPN implementation, provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners via the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dialup Internet access can securely and easily access your network resources with the SonicWALL Global VPN Client or Global Security Client and SonicWALL GroupVPN on your SonicWALL. Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to- network VPN connections.

➲ **Cross Reference:** *For more information on the SonicWALL Global VPN Client, see the **SonicWALL Global VPN Client Administrator's Guide**. For more information on the SonicWALL Global Security Client, see the **SonicWALL Global Security Client Administrator's Guide**.*

SonicWALL's GroupVPN provides automatic VPN policy provisioning for SOnicWALL Global VPN Clients. The GroupVPN feature on the SonicWALL security appliance and the SonicWALL Global VPN Client (part of the Global security Client) dramatically streamline VPN deployment and management. Using SonicWALL's Client Policy Provisioning technology, you define the VPN policies for Global VPN Client users. This policy information automatically downloads from the SonicWALL security appliance (VPN Gateway) to Global VPN Clients, saving remote users the burden of provisioning VPN connections.

You can easily and quickly create a site-to-site VPN policy or a GroupVPN policy for SonicWALL Global Security Clients using the **VPN Policy Wizard**. You can also configure GroupVPN or site-to-site VPN tunnels using the Management Interface. You can define up to four GroupVPN policies, one for each Zone. You can also create multiple site-to-site VPN. The maximum number of policies you can add depends on your SonicWALL model.

The **VPN>Settings** page provides the SonicWALL features for configuring your VPN policies. You configure site-to-site VPN policies and GroupVPN policies from this page.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
VPN Policy Wizard...
Apply
Cancel
?
Add...
Delete
Delete All

VPN > Settings

VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier: 0006B11247D6

VPN Policies

Items 1 to 4 (of 4)

☐ # Name	Gateway	Destinations	Crypto Suite	Enable	Configure
☐ 1 WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	
☐ 2 LAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	
☐ 3 DMZ GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	
☐ 4 WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	

4 Policies Defined, 0 Policies Enabled, 4001 Maximum Policies Allowed

Currently Active VPN Tunnels

Items 0 to 0 (of 0)

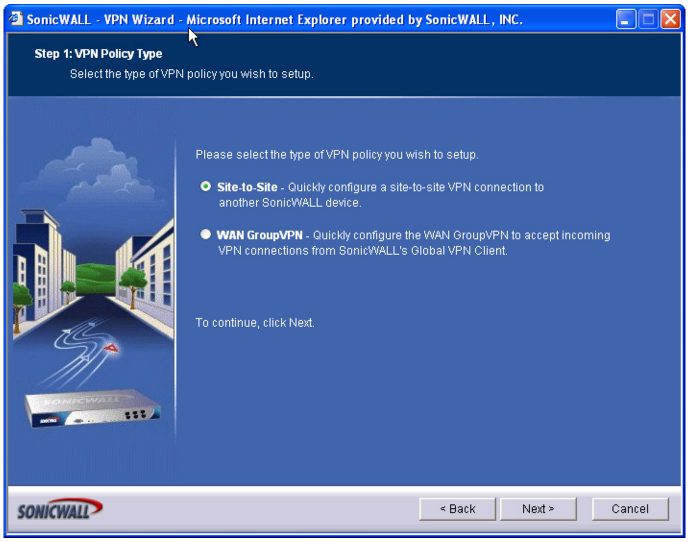
#	Name	Local	Remote	Gateway
No Entries				

Status: Ready

VPN Policy Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN or site-to-site VPN policies on the SonicWALL security appliance. After completing the configuration, the wizard creates the necessary VPN settings for the selected policy. You can use the SonicWALL Management Interface for optional advanced configuration options.

Cross Reference: *For step-by-step instructions on using the VPN Policy Wizard, see Chapter 50 Configuring VPNs with the VPN Policy Wizard.*


SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 1: VPN Policy Type

Select the type of VPN policy you wish to setup.

Please select the type of VPN policy you wish to setup.

● **Site-to-Site** - Quickly configure a site-to-site VPN connection to another SonicWALL device.

○ **WAN GroupVPN** - Quickly configure the WAN GroupVPN to accept incoming VPN connections from SonicWALL's Global VPN Client.

To continue, click Next.

VPN Global Settings

The **Global VPN Settings** section displays the following information:

- **Enable VPN** must be selected to allow VPN policies through the SonicWALL security policies.
- **Unique Firewall Identifier** - the default value is the serial number of the SonicWALL. You can change the Identifier, and use it for configuring VPN tunnels.

VPN Policies

All existing VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:

- **Name**: Displays the default name or user-defined VPN policy name.
- **Gateway**: Displays the IP address of the remote SonicWALL. If 0.0.0.0 is used, no Gateway is displayed.
- **Destinations**: Displays the IP addresses of the destination networks.
- **Crypto Suite**: Displays the type of encryption used for the VPN policy.
- **Enable**: Selecting the check box enables the VPN Policy. Clearing the check box disables it.
- **Configure**: Clicking the Edit icon allows you to edit the VPN policy. Clicking the Trashcan allows you to delete the VPN policy. The predefined GroupVPN policies cannot be deleted, so the Trashcan icons are dimmed. GroupVPN policies also have a Disk icon for exporting the VPN policy configuration as a file for local installation by SonicWALL Global VPN Clients.

The number of VPN policies defined, policies enabled, and the maximum number of Policies allowed is displayed below the table. You can define up to 4 GroupVPN policies, one for each Zone. These GroupVPN policies are listed by default in the VPN Policies table as **WAN GroupVPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. Clicking on the Edit icon in the Configure column for the GroupVPN displays the **VPN Policy** window for configuring the GroupVPN policy.

Below the VPN Policies table are the following buttons:

- **Add** - Accesses the **VPN Policy** window to configure site-to-site VPN policies.
- **Delete** - Deletes the selected (checked box before the VPN policy name in the **Name** column. You cannot delete the GroupVPN policies.
- **Delete All** - Deletes all VPN policies in the VPN Policies table except the default GroupVPN policies.

Navigating and Sorting the VPN Policies Entries

The **VPN Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **VPN Policies** table by using the navigation control bar located at the top right of the **VPN Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System>Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Currently Active VPN Tunnels

A list of currently active VPN tunnels is displayed in this section. The table lists the name of the VPN Policy, the local LAN IP addresses, and the remote destination network IP addresses as well as the peer gateway IP address.

Configuring GroupVPN Policies

SonicWALL **GroupVPN** facilitates the set up and deployment of multiple SonicWALL Global VPN Clients by the SonicWALL security appliance administrator. **GroupVPN** is only available for SonicWALL Global VPN Clients and it is recommended you use XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.

➲ **Cross Reference:** *For more information on the SonicWALL Global VPN Client, see the* ***SonicWALL Global VPN Client Administrator's Guide****. For more information on the SonicWALL Global Security Client, see the* ***SonicWALL Global Security Client Administrator's Guide****.*

The default GroupVPN configuration allows you to support SonicWALL Global VPN Clients without any further editing of the VPN policy, except to check the **Enable** box for GroupVPN in the **VPN Policies** table.

SonicWALL supports four GroupVPN policies. You can create GroupVPN policies for the DMZ, LAN, WAN, and WLAN zones. These GroupVPN policies are listed in the VPN policies tables as **WAN Group VPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. For these GroupVPN policies, you can choose from **IKE using Preshared Secret** or **IKE using 3rd Party Certificates** for your IPSec Keying Mode.

✓ **Tip:** *You can easily create GroupVPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see Chapter 51 Configuring VPNS with the VPN Policy Wizard.*

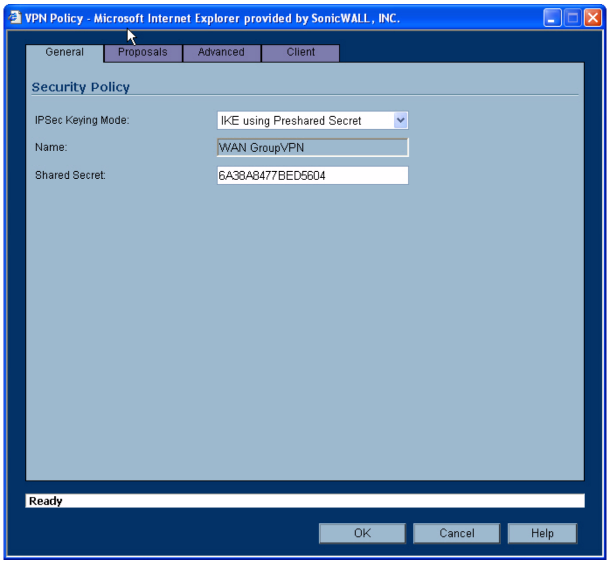
The following instructions explain configuring GroupVPN using the SonicWALL Management Interface.

➲ **Cross Reference:** *See the* ***GroupVPN Setup in SonicOS Enhanced*** *technote on the SonicWALL documentation Web site http://www.sonicwall.com for more GroupVPN configuration information.*

Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone

To configure the WAN GroupVPN, follow these steps:

1. Click the Edit icon for the **WAN GroupVPN** entry. The **VPN Policy** window is displayed.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

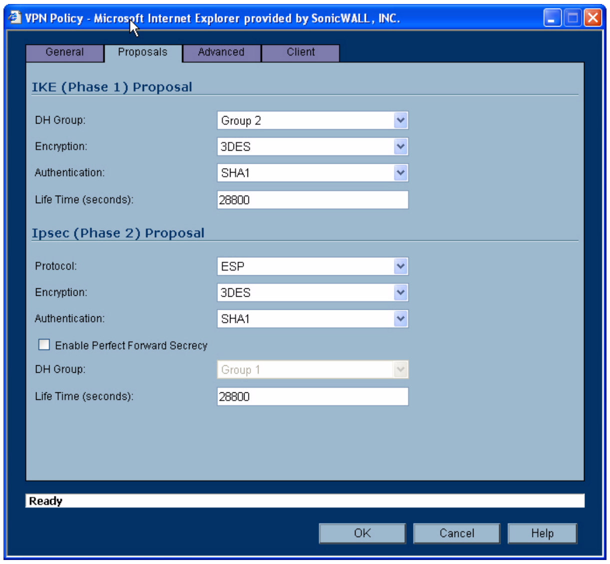
Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: WAN GroupVPN

Shared Secret: 6A38A8477BED5604

2. In the **General** tab, **IKE using Preshared Secret** is the default setting for **IPSec Keying Mode**. A Shared Secret is automatically generated by the SonicWALL security appliance in the **Shared Secret** field, or you can generate your own shared secret. **Shared Secrets** must be minimum of four characters. You cannot change the name of any GroupVPN policy.
3. Click the **Proposals** tab to continue the configuration process.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

IKE (Phase 1) Proposal

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

DH Group: Group 1

Life Time (seconds): 28800

In the **IKE (Phase 1) Proposal** section, use the following default settings:

Group 2 from the **DH Group** menu

3DES from the **Encryption** menu

SHA1 from the **Authentication** menu

Leave the default setting, **28800**, in the **Life Time (secs)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

In the **IPSec (Phase 2) Proposal** section, select the following default settings:

ESP from the **Protocol** menu

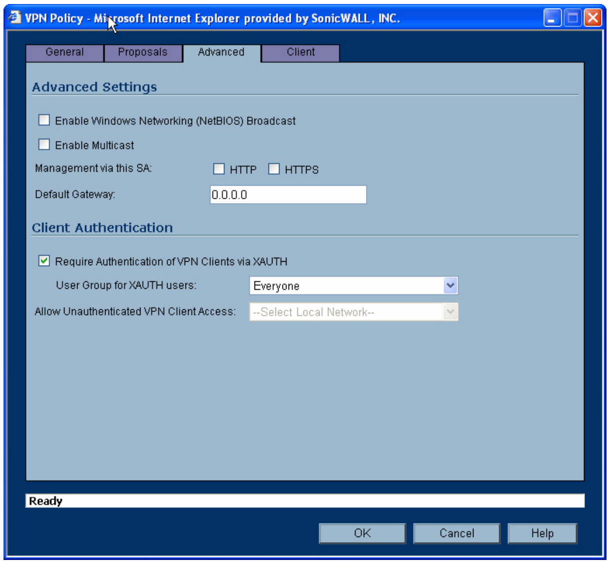
3DES from the **Encryption** menu

SHA1 from the **Authentication** menu

Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.

Leave the default setting, 28800, in the **Life Time (secs)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

4 Click the **Advanced** tab.



☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

Management via this SA: ☐ HTTP ☐ HTTPS

Default Gateway: 0.0.0.0

☑ Require Authentication of VPN Clients via XAUTH

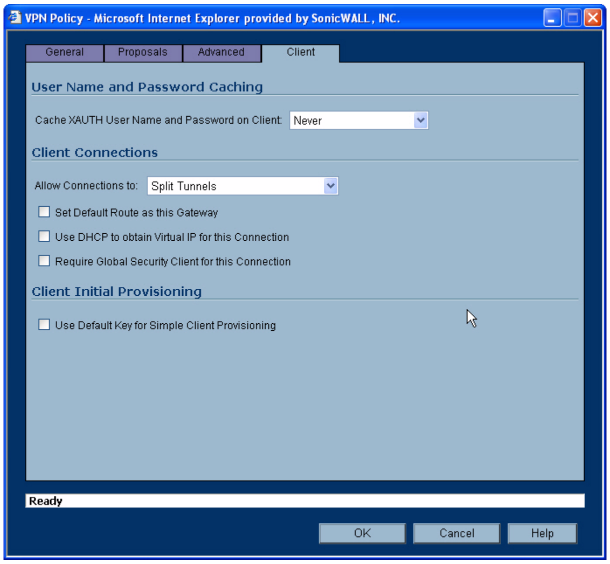
User Group for XAUTH users: Everyone

Allow Unauthenticated VPN Client Access: --Select Local Network--

Select any of the following optional settings you want to apply to your GroupVPN policy:

- **Enable Windows Networking (NetBIOS) broadcast** - allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Management via this SA**: - If using the VPN policy to manage the SonicWALL security appliance, select the management method, either **HTTP** or **HTTPS**.
- **Default Gateway** - allows the network administrator to specify the IP address of the default network route for incoming IPSec packets for this VPN policy. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL security appliance. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route. If no route is found, the security appliance checks for a Default Gateway. If a Default Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **Require Authentication of VPN Clients via XAUTH** - requires that all inbound traffic on this VPN tunnel is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel. he **Trusted users** group is selected by default. You can select another user group or **Everyone** from **User Group for XAUTH users**.
- **Allow Unauthenticated VPN Client Access** - allows you to enable unauthenticated VPN client access. If you uncheck **Require Authentication of VPN Clients via XAUTH**, the **Allow Unauthenticated VPN Client Access** menu is activated. Select an Address Object or Address Group from menu of predefined options, or select **Create new addess object** or **Create new address group** to create a new one.

5 Click the **Client** tab, select any of the following settings you want to apply to your GroupVPN policy.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Client
Ready
OK
Cancel
Help

User Name and Password Caching

Cache XAUTH User Name and Password on Client: Never

Client Connections

Allow Connections to: Split Tunnels

☐ Set Default Route as this Gateway

☐ Use DHCP to obtain Virtual IP for this Connection

☐ Require Global Security Client for this Connection

Client Initial Provisioning

☐ Use Default Key for Simple Client Provisioning

- **Cache XAUTH User Name and Password on Client** - allows the Global VPN Client to cache the user name and password.
  - **Never** - Global VPN Client is not allowed to cache the username and password. The user will be prompted for a username and password when the connection is enabled, and also every time there is an IKE Phase 1 rekey.
  - **Single Session** - Global VPN Client user prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey.
  - **Always** - Global VPN Client user prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
  - This Gateway Only - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
  - **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
  - **Split Tunnels** - Allows the VPN user to have both local Internet connecivity and VPN connectivity.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this VPN tunnel. You can only configure one VPN policy to use this setting.
- **Use DHCP to obtain Virtual IP for this Connection** - allows the VPN Client to obtain an IP address using DHCP over VPN.

- **Require Distributed Security Client for this Connection** - only allows a VPN connection from a remote computer running the SonicWALL Distributed Security Client, which provides policy enforced firewall protection before allowing a Global VPN Client connection.

Note: *For more information on the SonicWALL Global Security Client and Distributed Security Client, see the SonicWALL Global Security Client Administrator's Guide.*

- **Use Default Key for Simple Client Provisioning** - uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

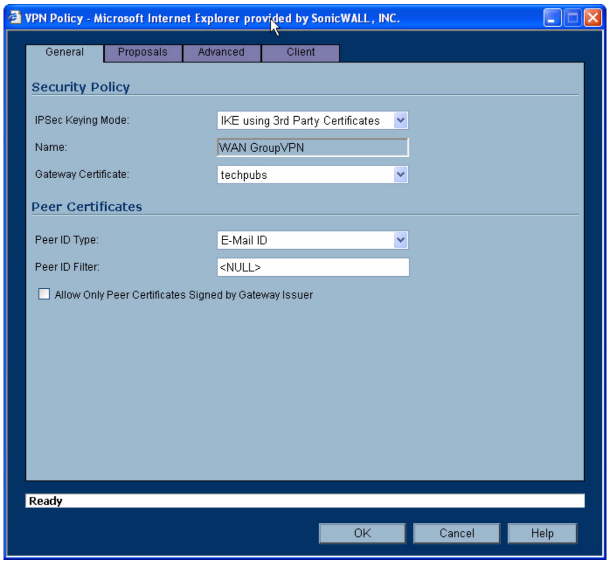
6 Click **OK**.

Configuring GroupVPN with IKE using 3rd Party Certificates

To configure GroupVPN with IKE using 3rd Party Certificates, follow these steps:

Alert: *Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the SonicWALL.*

1 In the **VPN>Settings** page click the **Notepad** icon under **Configure**. The **VPN Policy** window is displayed.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.

Security Policy

IPSec Keying Mode: IKE using 3rd Party Certificates

Name: WAN GroupVPN

Gateway Certificate: techpubs

Peer Certificates

Peer ID Type: E-Mail ID

Peer ID Filter: <NULL>

☐ Allow Only Peer Certificates Signed by Gateway Issuer

Ready

2 In the **Security Policy** section, select **IKE using 3rd Party Certificate**s from the **IPSec Keying Mode** menu. The VPN policy name is **GroupVPN** by default and cannot be changed.

3 Select a certificate for the SonicWALL from the **Gateway Certificate** menu.

4 Select one of the following Peer ID types from the **Peer ID Type** menu.

E-Mail ID

Distinguished name

Domain name

5 Enter the Peer ID filter in the **Peer ID Filter** field.

6 Check **Allow Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the **Gateway Certificate** menu.

7 Click on the **Proposals** tab.

8 In the **IKE (Phase 1) Proposal** section, select the following settings:

Group 2 from the **DH Group** menu.

3DES from the **Encryption** menu.

SHA1 from the **Authentication** menu.

Leave the default setting, **28800**, in the **Life Time (seconds)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

9 In the **IPSec (Phase 2) Proposal** section, select the following settings:

ESP from the **Protocol** menu.

3DES from the **Encryption** menu.

MD5 from the **Authentication** menu.

Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Then select **Group 2** from the **DH Group** menu.

Leave the default setting, **28800**, in the **Life Time (seconds)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

10 Click on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN Policy:

- **Enable Windows Networking (NetBIOS) broadcast** - allows access to remote network resources by browsing the Windows Network Neighborhood.
- **Management via this SA** - select HTTP and/or HTTPS.
- **Default LAN Gateway** - used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** check box. Default LAN Gateway allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **Require Authentication of VPN Clients via XAUTH** - requires that all inbound traffic on this VPN policy is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.
- **User group for XAUTH users** - allows you to select a defined user group for authentication.
- **All Unauthenticated VPN Client Access** - allows you to specify network segments for unauthenticated Global VPN Client access.

11 Click on the **Client** tab and select any of the following boxes that you want to apply to Global VPN Client provisioning:

- **Cache XAUTH User Name and Password** - allows the Global VPN Client to cache the user name and password. Select from:
  - **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
  - **Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
  - **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Allow Connection to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway. Select from **Split Tunnels**, **This Gateway Only**, or **All Secured Gateways**.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting.

- **Use DHCP to obtain Virtual IP for this Connection** - allows the VPN Client to obtain an IP address using DHCP over VPN.
- **Require Distributed Security Client for this Connection** - only allows a VPN connection from a remote computer running the SonicWALL Distributed Security Client, which provides policy enforced firewall protection before allowing a Global VPN Client connection.

Note: *For more information on the SonicWALL Global Security Client and Distributed Security Client, see the SonicWALL Global Security Client Administrator's Guide.*

- **Use Default Key for Simple Client Provisioning** - uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

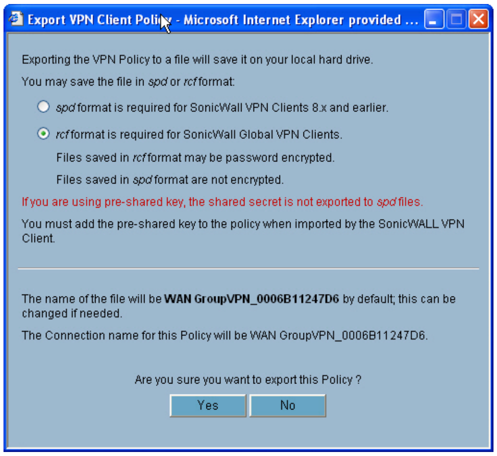
12 Click **OK**.

Exporting a VPN Client Policy

If you want to export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients, follow these instructions:

Alert: *The GroupVPN SA must be enabled on the SonicWALL to export a configuration file.*

1 Click the **Disk** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table. The **Export VPN Client Policy** window appears.


Export VPN Client Policy - Microsoft Internet Explorer provided ...

Exporting the VPN Policy to a file will save it on your local hard drive.

You may save the file in *spd* or *rcf* format:

○ *spd* format is required for SonicWall VPN Clients 8.x and earlier.

● *rcf* format is required for SonicWall Global VPN Clients.

Files saved in *rcf* format may be password encrypted.

Files saved in *spd* format are not encrypted.

If you are using pre-shared key, the shared secret is not exported to *spd* files.

You must add the pre-shared key to the policy when imported by the SonicWALL VPN Client.

The name of the file will be **WAN GroupVPN_0006B11247D6** by default; this can be changed if needed.

The Connection name for this Policy will be WAN GroupVPN_0006B11247D6.

Are you sure you want to export this Policy ?

2 **rcf format is required for SonicWALL Global Clients** is selected by default. Files saved in the rcf format can be password encrypted. The SonicWALL provides a default file name for the configuration file, which you can change.

3 Click **Yes**. The **VPN Policy Export** window appears.

4 Type a password in the **Passwor**d field and reenter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.

5 Click **Submit**. If you did not enter a password, a message appears confirming your choice.

6 Click **OK**. You can change the configuration file before saving.

7 Save the file.

8 Click **Close**.

The file can be saved to a floppy disk or sent electronically to remote users to configure their Global VPN Clients.

Site-to-Site VPN Configurations

When designing VPN connections, be sure to document all pertinent IP Addressing information and create a network diagram to use as a reference. A sample planning sheet is provided on the next page. The SonicWALL must have a routable WAN IP Address whether it is dynamic or static. In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

Site-to-Site VPN configurations can include the following options:

- **Branch Office (Gateway to Gateway)** - A SonicWALL is configured to connect to another SonicWALL via a VPN tunnel. Or, a SonicWALL is configured to connect via IPSec to another manufacturer's firewall.
- **Hub and Spoke Design** - All SonicWALL VPN gateways are configured to connect to a central SonicWALL (hub), such as a corporate SonicWALL. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a SonicWALL.
- **Mesh Design** - All sites connect to all other sites. All sites must have static IP addresses.

VPN Planning Sheet for Site-to-Site VPN Policies

You need the information below before you begin configuring Site-to-Site VPN Policies.

Site A

Workstation

LAN IP Address: ___.___.___.___

Subnet Mask: ___.___.___.___

Default Gateway: ___.___.___.___

SonicWALL

LAN IP Address: ___.___.___.___

WAN IP Address: ___.___.___.___

Subnet Mask: ___.___.___.___

Default Gateway: ___.___.___.___

Router

Internet Gateway

WAN IP Address: ___.___.___.___

Subnet Mask: ___.___.___.___

DNS Server #1: ___.___.___.___

DNS Server #2: ___.___.___.___

Additional Information

SA Name:____________________

Manual Key, SPI In_____ SPI Out_____

Enc.Key:____________________

Auth.Key:___________________

If Preshared Secret,

Shared Secret:___________________

Local IKE ID and Remote IKE ID

Phase 1 DH - 1 2 5

SA Lifetime 28800 or ____________

Phase 1 Enc/Auth DES 3DES AES-128 AES-256 MD5 SHA1 (circle)

Phase 2 Enc/Auth DES 3DES AES-128 AES-256 MD5 SHA1 (circle)

ARC NULL

Local Network in a VPN Policy

__ Choose local network from list

__ Local network obtains IP addresses using DHCP through this VPN tunnel

__ Any address

Remote Networks

__ Use this VPN tunnel as a default route for all Internet traffic

__ Destination network obtains address using DHCP through this VPN tunnel

__ Choose destination network from list

Primary IPSec Gateway/Secondary IPSec Gateway

Creating Site-to-Site VPN Policies

You can create or modify existing VPN policies using the VPN Policy window. Clicking the **Add** button under the **VPN Policies** table displays the **VPN Policy** window for configuring the following IPSec Keying mode VPN policies:

- IKE using Preshared Key
- Manual Key
- IKE using 3rd Party Certificates

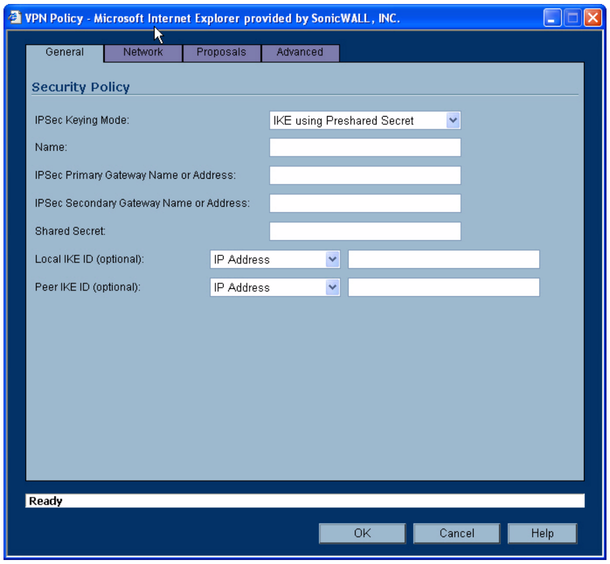
✓ **Tip:** *Use the VPN Planning Sheet for Site-to-Site VPN Policies to record your settings. These settings are necessary to configure the remote SonicWALL and create a successful VPN connection.*

➲ **Cross Reference:** *For configuring VPN policies between SonicWALL security appliances running SonicOS Enhanced and SonicWALL security appliances running SonicWALL Firmware version 6.5 (or higher), see the technote: Creating IKE IPSec VPN Tunnels between SonicWALL Firmware 6.5 and SonicOS Enhanced, available at the SonicWALL documentation Web site http://www.sonicwall.com/services/documentation.html.*

Configuring a VPN Policy with IKE using Preshared Secret

To configure a VPN Policy using Internet Key Exchange (IKE), follow the steps below:

1 Click **Add** on the **VPN>Settings** page. The **VPN Policy** window is displayed.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Security Policy
Name:
IPSec Primary Gateway Name or Address:
IPSec Secondary Gateway Name or Address:
Shared Secret:
Ready
OK
Cancel
Help

IPSec Keying Mode: IKE using Preshared Secret

Local IKE ID (optional): IP Address

Peer IKE ID (optional): IP Address

2 In the **General** tab, select **IKE using Preshared Secret** from the **IPSec Keying Mode** menu.

3 Enter a name for the policy in the **Name** field.

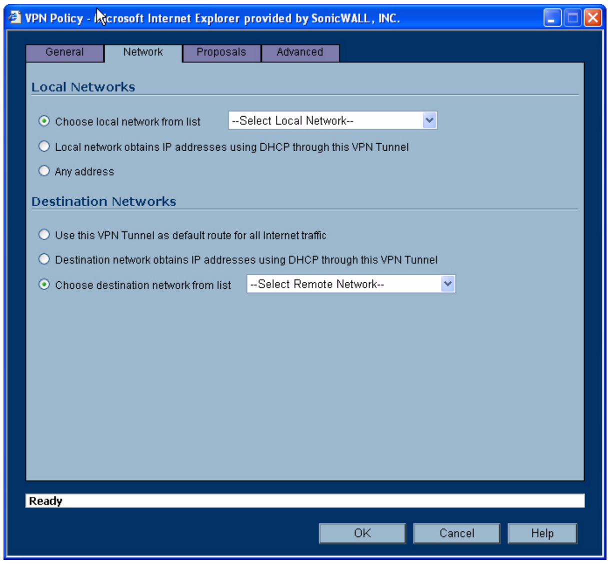
4 Enter the host name or IP address of the remote connection in the **IPSec Primary Gateway Name or Address** field.

5 If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPSec Secondary Gateway Name or Address** field.

6 Enter a Shared Secret password to be used to setup the Security Association the **Shared Secret** field. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

Optionally, specify a **Local IKE ID (optional)** and **Peer IKE ID (optional)** for this Policy. By default, the IP Address (ID_IPv4_ADDR) is used for Main Mode negotiations, and the SonicWALL Identifier (ID_USER_FQDN) is used for Aggressive Mode.

7 Click the **Network** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Local Networks
Destination Networks
Ready
OK
Cancel
Help

● Choose local network from list --Select Local Network--

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

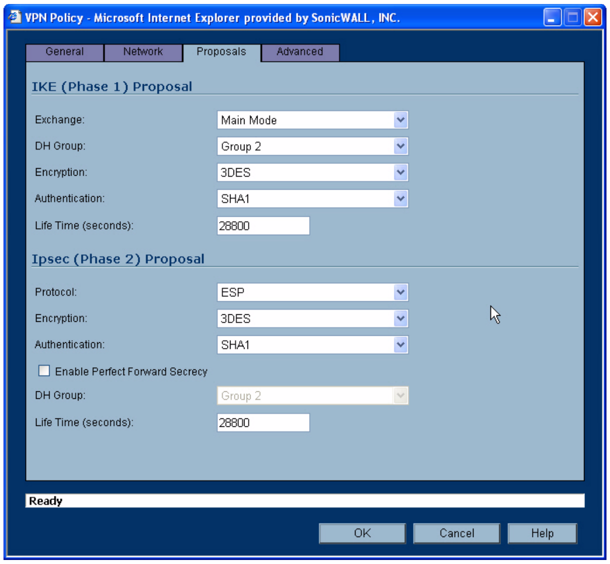
○ Any address

○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Choose destination network from list --Select Remote Network--

8. Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected.
9. Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if all remote VPN connections access the Internet through this SA. Traffic from any local use cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.
10. Click **Proposals**.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

IKE (Phase 1) Proposal

Exchange: Main Mode
DH Group: Group 2
Encryption: 3DES
Authentication: SHA1
Life Time (seconds): 28800

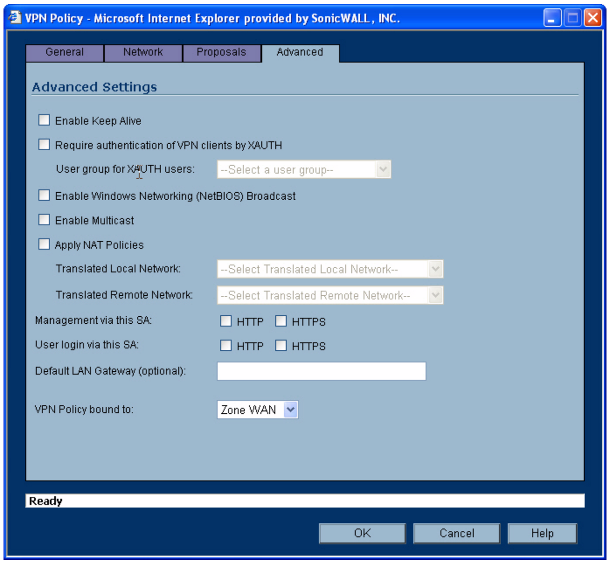
Ipsec (Phase 2) Proposal

Protocol: ESP
Encryption: 3DES
Authentication: SHA1
☐ Enable Perfect Forward Secrecy
DH Group: Group 2
Life Time (seconds): 28800

Ready

11. Under **IKE (Phase 1) Proposal**, select either **Main Mode** or **Aggressive Mode** from the **Exchange** menu. **Aggressive Mode** is generally used when WAN addressing is dynamically assigned.
12. Under **IKE (Phase 1) Proposal**, the default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations. Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.
13. **Under IPSec (Phase 2) Proposal**, the default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, **DH Group**, and **Lifetime** are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

14 Click **Advanced**.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

Advanced Settings

☐ Enable Keep Alive

☐ Require authentication of VPN clients by XAUTH

User group for XAUTH users: --Select a user group--

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

☐ Apply NAT Policies

Translated Local Network: --Select Translated Local Network--

Translated Remote Network: --Select Translated Remote Network--

Management via this SA: ☐ HTTP ☐ HTTPS

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

Ready

15 Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep Alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.

16 To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.

17 Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

18 Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.

19 Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

20 To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.

21 If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

22 Select an interface or Zone from the **VPN Policy bound to** menu. A WAN Zone is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

23 Click OK.

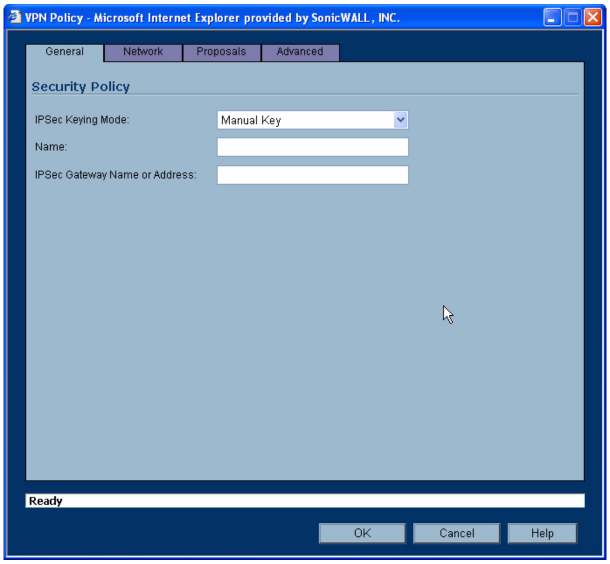
24 Click Apply on the **VPN>Settings** page to update the VPN Policies.

Configuring a VPN Policy using Manual Key

To manually configure a VPN policy between two SonicWALL appliances using Manual Key, follow the steps below:

Local SonicWALL

1 Click **Add** on the **VPN>Settings** page. The **VPN Policy** window is displayed.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Security Policy
Ready
OK
Cancel
Help

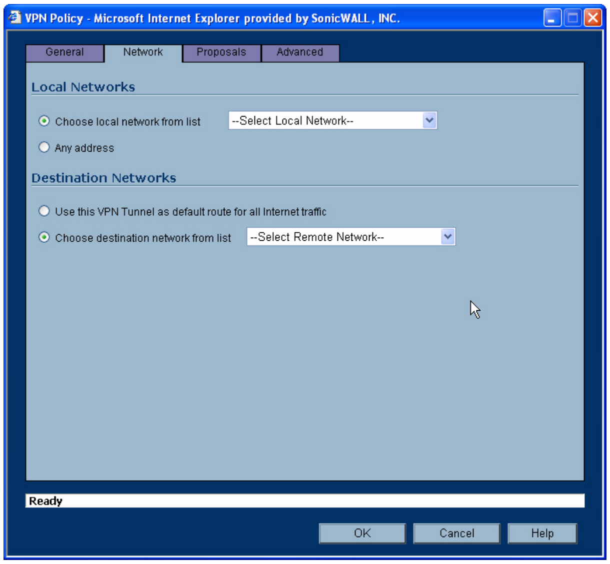
IPSec Keying Mode: Manual Key
Name:
IPSec Gateway Name or Address:

2 In the **General** tab, select **Manual Key** from the **IPSec Keying Mode** menu.

3 Enter a name for the policy in the **Name** field.

4 Enter the host name or IP address of the remote connection in the **IPSec Gateway Name or Address** field.

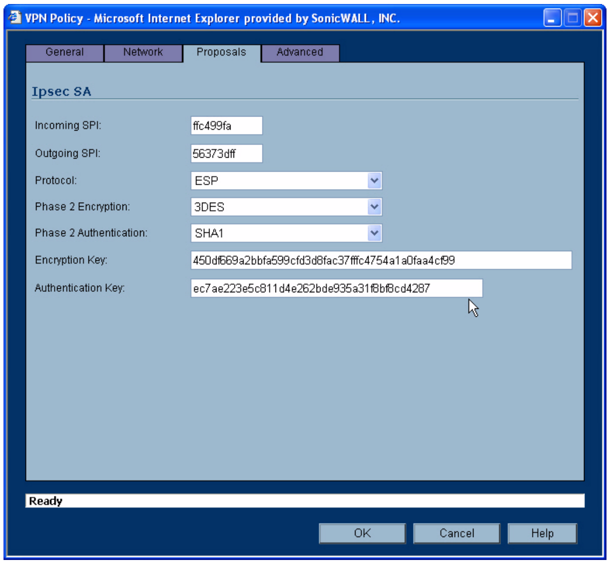
5 Click the **Network** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Local Networks
Destination Networks
Ready
OK
Cancel
Help

● Choose local network from list --Select Local Network--
○ Any address
○ Use this VPN Tunnel as default route for all Internet traffic
● Choose destination network from list --Select Remote Network--

6 Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Use this option is a peer has **Use this VPN Tunnel as default route for all Internet traffic** selected. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group.

7. Click on the **Proposals** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Ready
OK
Cancel
Help

Ipsec SA

Incoming SPI: ffc499fa

Outgoing SPI: 56373dff

Protocol: ESP

Phase 2 Encryption: 3DES

Phase 2 Authentication: SHA1

Encryption Key: 450df669a2bbfa599cfd3d8fac37fffc4754a1a0faa4cf99

Authentication Key: ec7ae223e5c811d4e262bde935a31f8bf8cd4287

8. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

Alert: *Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.*

9. The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.

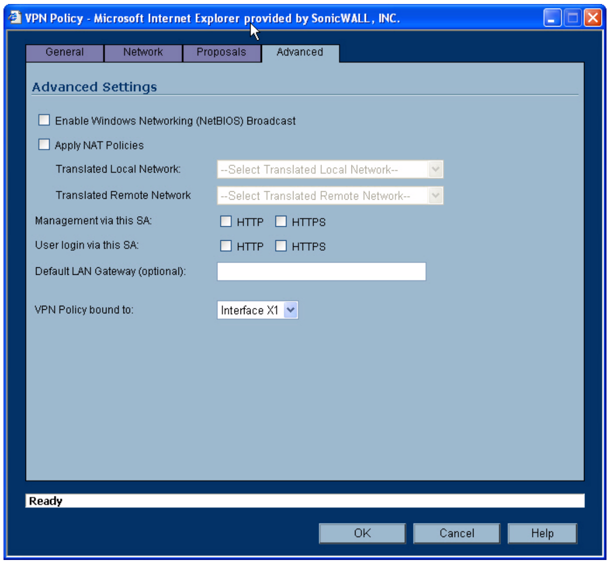
Note: *The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote SonicWALL.*

10. Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the SonicWALL.

11. Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the SonicWALL settings.

Tip: *Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a,b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.*

12 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.



VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.

General | Network | Proposals | Advanced

Advanced Settings

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Apply NAT Policies

Translated Local Network: --Select Translated Local Network--

Translated Remote Network: --Select Translated Remote Network--

Management via this SA: ☐ HTTP ☐ HTTPS

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Interface X1

Ready

Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

Select **Apply NAT Policies** if your want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA.**

Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.

If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.

Select an interface from the **VPN Policy bound to** menu.

13 Click **OK**.

14 Click **Apply** on the **VPN >Settings** page to update the VPN Policies.

Remote SonicWALL

1 Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.

2 In the **General** tab, select **Manual Key** from the **IPSec Keying Mode** menu.

3 Enter a name for the SA in the **Name** field.

4 Enter the host name or IP address of the local connection in the **IPSec Gateway Name or Address** field.

5 Click the **Network** tab.

6 Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select **Use this VPN Tunnel as default route for all Internet traffic** if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group.

7 Click the **Proposals** tab.

8. Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

Alert: *Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.*

9. The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.

Note: *The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote SonicWALL.*

10. Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the remote SonicWALL.

11. Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the remote SonicWALL settings.

Tip: *Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a,b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.*

12. Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.

    Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

    Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

Alert: *You cannot use this feature if you have selected **Use this VPN Tunnel as the default route for all Internet traffic** on the **Network** tab.*

    To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA.**

    Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.

    If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.

    Select an interface from the **VPN Policy bound to** menu.

13. Click **OK**.

14. Click **Apply** on the **VPN >Settings** page to update the VPN Policies.

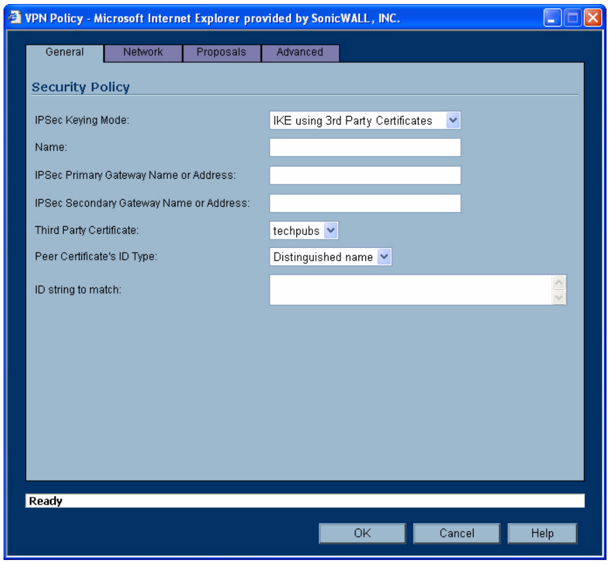
Tip: *Since Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.*

Configuring a VPN Policy with IKE using a Third Party Certificate

Alert: *You must have a valid certificate from a third party Certificate Authority installed on your SonicWALL before you can configure your VPN policy with IKE using a third party certificate.*

To create a VPN SA using IKE and third party certificates, follow these steps:

1 In the **VPN>Settings** page, click **Add**. The **VPN Policy** window is displayed.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Security Policy
Name:
IPSec Primary Gateway Name or Address:
IPSec Secondary Gateway Name or Address:
ID string to match:
Ready
OK
Cancel
Help

IPSec Keying Mode: IKE using 3rd Party Certificates

Third Party Certificate: techpubs

Peer Certificate's ID Type: Distinguished name

2 In **General** tab, select **IKE using 3rd Party Certificates**.

3 Type a Name for the Security Association in the **Name** field.

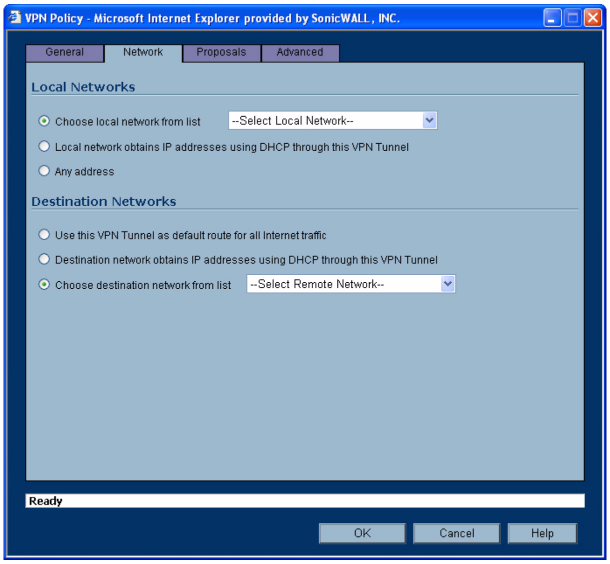
4 Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWALL in the **IPSec Primary Gateway Name or Address** field. If you have a secondary remote SonicWALL, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPSec Secondary Gateway Name or Address** field.

5 Select a certificate from the **Third Party Certificate** menu.

6 Select **Distinguished name**, **E-Mail ID**, or **Domain name** from the **Peer Certificate's ID Type** menu.

7 Type an ID string in the **ID string to match** field.

8 Click on the **Network** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

Local Networks

● Choose local network from list: --Select Local Network--

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

○ Any address

Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

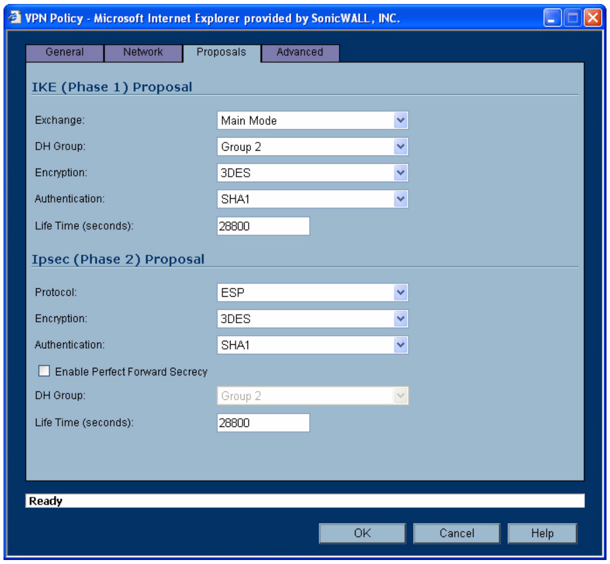
● Choose destination network from list: --Select Remote Network--

Ready

9 Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**.

10 Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.

11 Click the **Proposals** tab.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
OK
Cancel
Help

IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

DH Group: Group 2

Life Time (seconds): 28800

Ready

12 In the **IKE (Phase 1) Proposal** section, select the following settings:

Select **Aggressive Mode** from the **Exchange** menu.

Select **Group 2** from the **DH Group** menu.

Select **3DES** from the **Encryption** menu.

Enter a maximum time in seconds allowed before forcing the policy to renegotiate and exchange keys in the **Life Time** field. The default settings is **28800** seconds (8 hours).

13 In the **Ipsec (Phase 2) Proposal** section, select the following settings:

Select **ESP** from the **Protocol** menu.

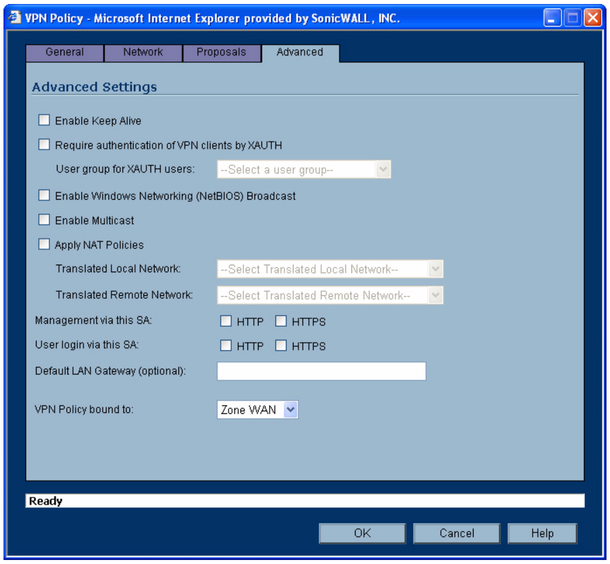
Select **3DES** from the **Encryption** menu.

Select **SHA1** from the **Authentication** menu.

Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security, then select **Group 2** from the **DH Group** menu.

Enter a maximum time in seconds allowed before forcing the policy to renegotiate and exchange keys in the **Life Time** field. The default settings is **28800** seconds (8 hours).

14 Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy in the **Advanced Settings** section.


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Network
Proposals
Advanced
Advanced Settings
Ready
OK
Cancel
Help

☐ Enable Keep Alive
☐ Require authentication of VPN clients by XAUTH
User group for XAUTH users: --Select a user group--
☐ Enable Windows Networking (NetBIOS) Broadcast
☐ Enable Multicast
☐ Apply NAT Policies
Translated Local Network: --Select Translated Local Network--
Translated Remote Network: --Select Translated Remote Network--
Management via this SA: ☐ HTTP ☐ HTTPS
User login via this SA: ☐ HTTP ☐ HTTPS
Default LAN Gateway (optional):
VPN Policy bound to: Zone WAN

Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep Alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.

To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.

Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.

If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

Select an interface or Zone from the **VPN Policy bound to** menu. A Zone is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

15 Click **OK**.

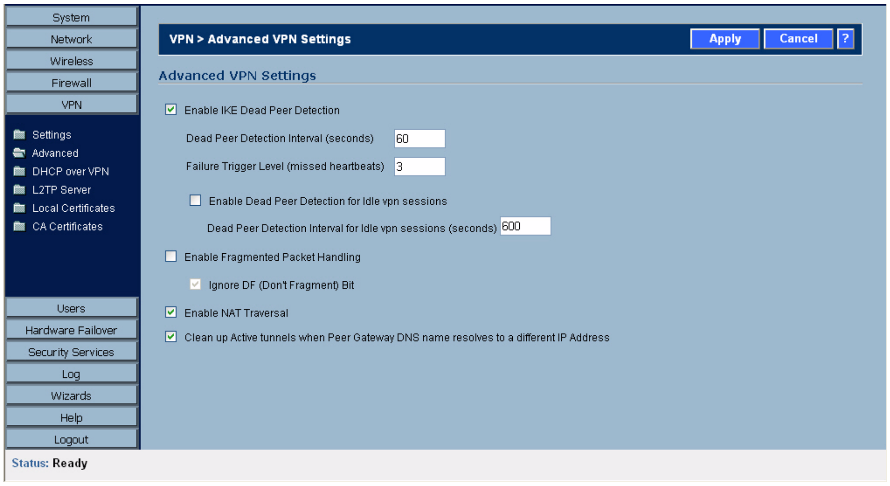
16 Click **Apply** on the **VPN>Settings** page to update the VPN Policies. Your new VPN policy is displayed in the **VPN Policies** table.

CHAPTER 30

Configuring Advanced VPN Settings

VPN>Advanced

The **Advanced VPN Settings** page includes optional settings that affect all VPN policies.


System
Network
Wireless
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
VPN > Advanced VPN Settings
Apply
Cancel
?

Advanced VPN Settings

☑ Enable IKE Dead Peer Detection

Dead Peer Detection Interval (seconds): 60

Failure Trigger Level (missed heartbeats): 3

☐ Enable Dead Peer Detection for Idle vpn sessions

Dead Peer Detection Interval for Idle vpn sessions (seconds): 600

☐ Enable Fragmented Packet Handling

☑ Ignore DF (Don't Fragment) Bit

☑ Enable NAT Traversal

☑ Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address

Status: Ready

Advanced VPN Settings

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the SonicWALL.

  Dead Peer Detection Interval - Enter the number of seconds between "heartbeats" in the **Dead peer detection Interval (seconds)** field. The default value is 60 seconds.

  Failure Trigger Level (missed heartbeats) - Enter the number of missed heartbeats in the **Failure Trigger Level (missed heartbeats)** field. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the SonicWALL security appliance. The SonicWALL security appliance uses a UDP packet protected by Phase 1 Encryption as the heartbeat.
- **Enable Dead Peer Detection for Idle VPN Sessions** - Select this setting if you want idle VPN connections to be dropped by the SonicWALL security appliance after the time value defined in the **Dead Peer Detection Interval for Idle VPN Sessions (seconds)** field. The default value is 600 seconds (10 minutes).

- **Enable Fragmented Packet Handling** - If the VPN log report shows the log message "Fragmented IPSec packet dropped", select this feature. Do not select it until the VPN tunnel is established and in operation.

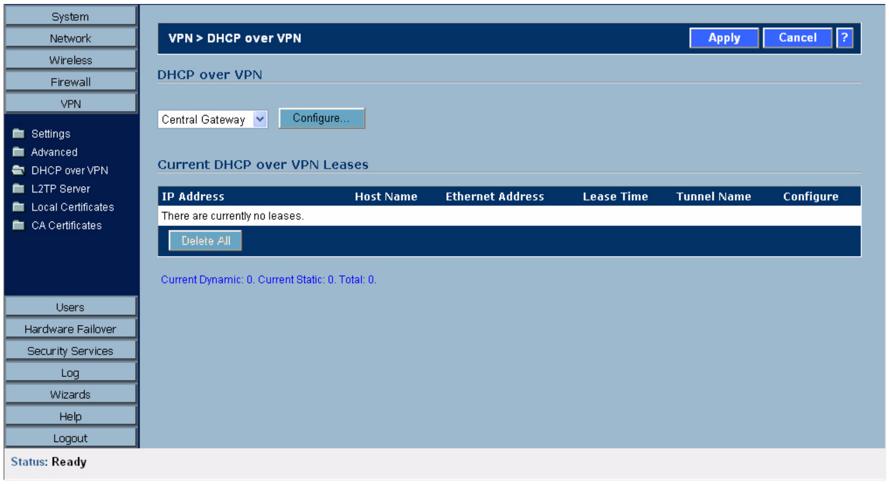
  Ignore DF (Don't Fragment) Bit - when you select **Enable Fragmented Packet Handling**, the **Ignore DF (Don't Fragment) Bit** setting becomes active.
- **Enable NAT Traversal** - Select this setting is a NAT device is located between your VPN endpoints. IPSec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPSec session, a 1-byte UDP is designated as a "NAT Traversal keepalive" and acts as a "heartbeat" sent by the VPN device behind the NAT or NAPT device. The "keepalive" is silently discarded by the IPSec peer.
- **Clean up Active Tunnels when Peer Gateway DNS names resolves to a different IP address** - Breaks down SAs associated with old IP addresses and reconnects to the peer gateway.

CHAPTER 31

Configuring DHCP Over VPN

VPN > DHCP over VPN

The **VPN > DHCP over VPN** page allows you to configure a Host (DHCP Client) behind a SonicWALL security appliance to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.


System
Network
Wireless
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
VPN > DHCP over VPN
Apply
Cancel
?
DHCP over VPN
Configure...
Current DHCP over VPN Leases
Delete All

Central Gateway

IP Address	Host Name	Ethernet Address	Lease Time	Tunnel Name	Configure
There are currently no leases.					

Current Dynamic: 0. Current Static: 0. Total: 0.

Status: Ready

DHCP Relay Mode

The SonicWALL security appliance at the remote and central site are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The SonicWALL security appliance at the remote site (**Remote Gateway**) passes DHCP broadcast packets through its VPN tunnel. The SonicWALL security appliance at the central site (**Central Gateway**) relays DHCP packets from the client on the remote network to the DHCP server on the central site.

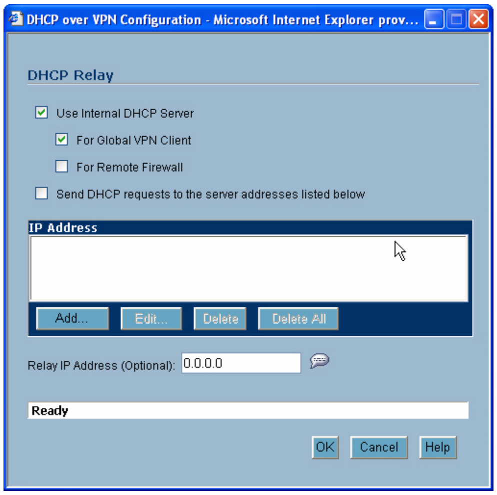
Configuring the Central Gateway for DHCP Over VPN

To configure **DHCP over VPN** for the **Central Gateway**, use the following steps:

1 Select **VPN>DHCP over VPN**.

2 Select **Central Gateway** from the **DHCP Relay Mode** menu.

3 Click **Configure**. The **DHCP over VPN Configuration** window is displayed.


DHCP over VPN Configuration - Microsoft Internet Explorer prov...
DHCP Relay
IP Address
Add...
Edit...
Delete
Delete All
OK
Cancel
Help

☑ Use Internal DHCP Server
☑ For Global VPN Client
☐ For Remote Firewall
☐ Send DHCP requests to the server addresses listed below

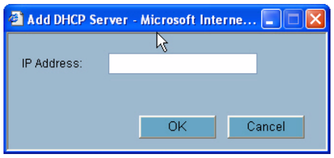
Relay IP Address (Optional): 0.0.0.0

Ready

4 Select **Use Internal DHCP Server** to enable the SonicWALL Global VPN Client or a remote firewall or both to use an internal DHCP server to obtain IP addressing information. Check the **For Global VPN Client** checkbox to use the DHCP Server for Global VPN Clients and check the **For Remote Firewall** checkbox for the SonicWALL Global Security Client's firewall.

5 If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.

6 Click **Add**. The **Add DHCP Server** window is displayed.


Add DHCP Server - Microsoft Interne...
IP Address:
OK
Cancel

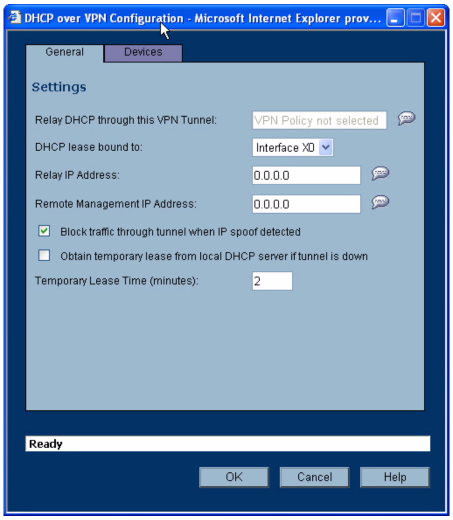
7 Type the IP addresses of DHCP servers in the **IP Address** field, and click **OK**. The SonicWALL security appliance now directs DHCP requests to the specified servers.

8 Type the IP address of a relay server in the **Relay IP Address (Optional)** field.

To edit an entry in the **IP Address** table, click **Edit.** To delete a DHCP Server, highlight the entry in the **IP Address** table, and click **Delete**. Click **Delete All** to delete all entries.

Configuring DHCP over VPN Remote Gateway

1. Select **Remote Gateway** from the **DHCP Relay Mode** menu.
2. Click **Configure**. The **DHCP over VPN Configuration** window is displayed.


DHCP over VPN Configuration - Microsoft Internet Explorer prov...
General
Devices
Settings
OK
Cancel
Help

Relay DHCP through this VPN Tunnel: VPN Policy not selected
DHCP lease bound to: Interface X0
Relay IP Address: 0.0.0.0
Remote Management IP Address: 0.0.0.0
☑ Block traffic through tunnel when IP spoof detected
☐ Obtain temporary lease from local DHCP server if tunnel is down
Temporary Lease Time (minutes): 2
Ready

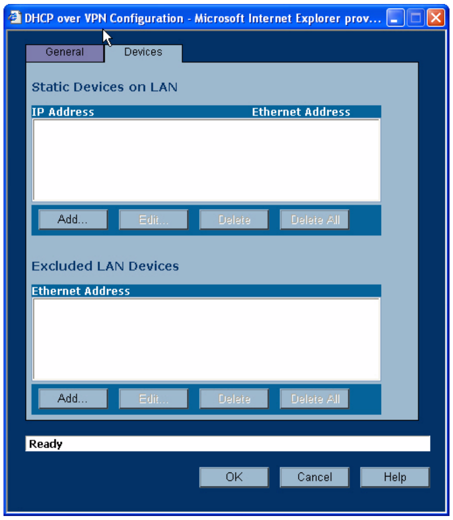
3. In the **General** tab, select the VPN policy to be used to relay DHCP requests from the Central Gateway. The VPN policy name is automatically displayed in the Relay DHCP through this VPN Tunnel filed if the VPN policy has the setting **Local network obtains IP addresses using DHCP through this VPN Tunnel** enabled.

Alert: *Only VPN policies using IKE can be used as VPN tunnels for DHCP.*

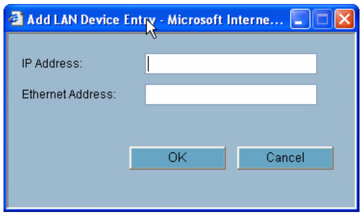
4. Select the interface the DHCP lease is bound from the **DHCP lease bound to** menu.
5. If you enter an IP address in the **Relay IP address** field, this IP address is used as the DHCP Relay Agent IP address in place of the Central Gateway's address, and must be reserved in the DHCP scope on the DHCP server. This address can also be used to manage this SonicWALL security appliance remotely through the VPN tunnel from behind the Central Gateway.
6. If you enter an IP address in the **Remote Management IP Address** field, this IP address is used to manage the SonicWALL security appliance from behind the Central Gateway, and must be reserved in the DHCP scope on the DHCP server.
7. If you enable **Block traffic through tunnel when IP spoof detected**, the SonicWALL security appliance blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is typed for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the SonicWALL security appliance to respond to IP spoofs.
8. If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. Enable the **Obtain temporary lease from local DHCP server if tunnel is down** check box. By enabling this check box, you have a failover option in case the tunnel ceases to function. If you want to allow temporary leases for a certain time period, type the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is 2 minutes.

Devices

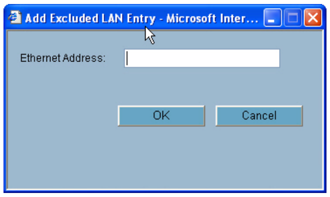
1 To configure devices on your LAN, click the **Devices** tab.


DHCP over VPN Configuration - Microsoft Internet Explorer prov...
General
Devices
Static Devices on LAN
IP Address
Ethernet Address
Add...
Edit...
Delete
Delete All
Excluded LAN Devices
Ethernet Address
Add...
Edit...
Delete
Delete All
Ready
OK
Cancel
Help

2 To configure **Static Devices on the LAN**, click **Add** to display the **Add LAN Device Entry** window, and type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field. An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to type the Ethernet address of a device. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses. Click **OK**.


Add LAN Device Entry - Microsoft Interne...
IP Address:
Ethernet Address:
OK
Cancel

3 To exclude devices on your LAN, click **Add** to display the **Add Excluded LAN Entry** window. Enter the MAC address of the device in the **Ethernet Address** field. Click **OK**.


Add Excluded LAN Entry - Microsoft Inter...
Ethernet Address:
OK
Cancel

4 Click **OK** to exit the **DHCP over VPN Configuration** window.

▲ **Alert:** *You must configure the local DHCP server on the remote SonicWALL security appliance to assign IP leases to these computers.*

▲ **Alert:** *If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.*

✓ **Tip:** *If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, i.e. two LANs.*

Current DHCP over VPN Leases

The scrolling window shows the details on the current bindings: IP and Ethernet address of the bindings, along with the Lease Time, and Tunnel Name. To edit an entry, click the Notepad icon under **Configure** for that entry.

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the Trashcon icon. The operation takes a few seconds to complete. Once completed, a message confirming the update is displayed at the bottom of the Web browser window.

Click **Delete All** to delete all VPN leases.

CHAPTER 32

Configuring L2TP Server

VPN > L2TP Server

The SonicWALL security appliance can terminate L2TP-over-IPSec connections from incoming Microsoft Windows 2000 and Windows XP clients. In situations where running the SonicWALL Global VPN Client is not possible, you can use the SonicWALL L2TP Server to provide secure access to resources behind the SonicWALL security appliances.

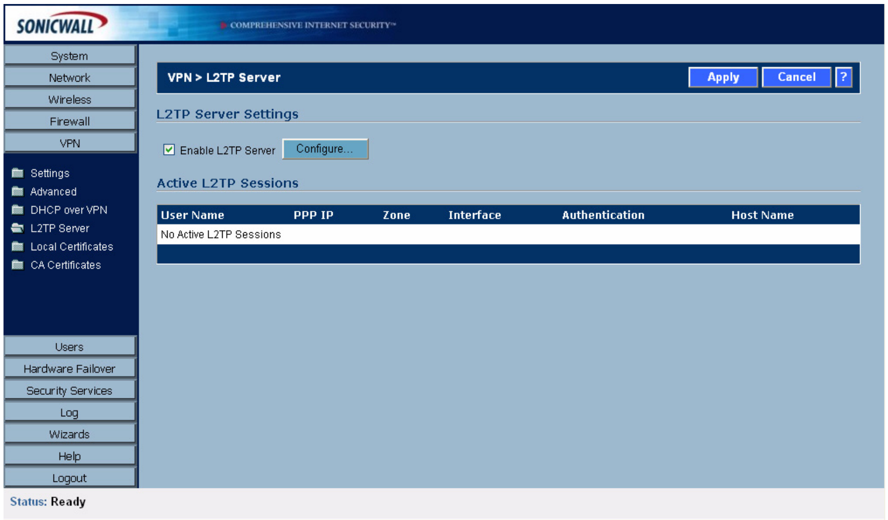
You can use Layer 2 Tunneling Protocol (L2TP) to create VPN over public networks such as the Internet. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them. L2TP is supported on Microsoft Windows 2000 Operating System.

L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPSec to provide a secure, encrypted VPN solution.

➲ **Cross Reference:** For more complete information on configuring the L2TP Server, see the technote **Configuring the L2TP Server in SonicOS** located on the SonicWALL documentation site: http://www.sonicwall.com/services/documentation.htm.

Configuring the L2TP Server

The **VPN > L2TP Server** page provides the settings for configuring the SonicWALL security appliance as a LT2P Server.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Configure...

VPN > L2TP Server

L2TP Server Settings

☑ Enable L2TP Server

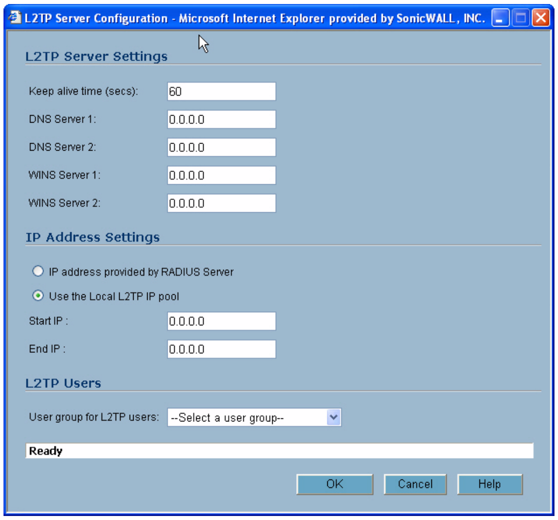
Active L2TP Sessions

User Name	PPP IP	Zone	Interface	Authentication	Host Name
No Active L2TP Sessions					

Status: Ready

To configure the L2TP Server, follow these steps:

1. To enable L2TP Server functionality on the SonicWALL security appliance, select **Enable L2TP Server**. Then click **Configure** to display the **L2TP Server Configuration** window.


L2TP Server Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
OK
Cancel
Help

L2TP Server Settings

Keep alive time (secs): 60
DNS Server 1: 0.0.0.0
DNS Server 2: 0.0.0.0
WINS Server 1: 0.0.0.0
WINS Server 2: 0.0.0.0

IP Address Settings

○ IP address provided by RADIUS Server
● Use the Local L2TP IP pool
Start IP : 0.0.0.0
End IP : 0.0.0.0

L2TP Users

User group for L2TP users: --Select a user group--

Ready

2. Enter the number of seconds in the **Keep alive time (secs)** field to send special packets to keep the connection open. The default is **60** seconds.
3. Enter the IP address of your first DNS server in the **DNS Server 1** field. If you have a second DNS server, type the IP address in the **DNS Server 2** field.
4. Enter the IP address of your first WINS server in the **WINS Server 1** field. If you have a second WINS server, type the IP address in the **WINS Server 2** field.
5. Select **IP address provided by RADIUS Server** if a RADIUS Server provides IP addressing information to the L2TP clients.
6. If the L2TP Server provides IP addresses, select **Use the Local L2TP IP** pool. Enter the range of private IP addresses in the **Start IP** and **End IP** fields. The private IP addresses should be a range of IP addresses on the LAN.

7 If you have configured a specific user group defined for using L2TP, select it from the **User Group for L2TP users** menu or use **Everyone**.

8 Click **OK**.

Currently Active L2TP Sessions

- **User Name** - the user name assigned in the local user database or the RADIUS user database.
- **PPP IP** - the source IP address of the connection.
- **Zone** - the zone used by the LT2P client.
- **Interface** - the type of interface used to access the L2TP Server, whether it's a VPN client or another SonicWALL security appliance.
- **Authentication** - type of authentication used by the L2TP client.
- **Host Name** - the name of the network connecting to the L2TP Server.

CHAPTER

33

Configuring VPN Certificates

VPN>CA Certificates

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWALL has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange VPN policy. IKE is an important part of IPSec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs. Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

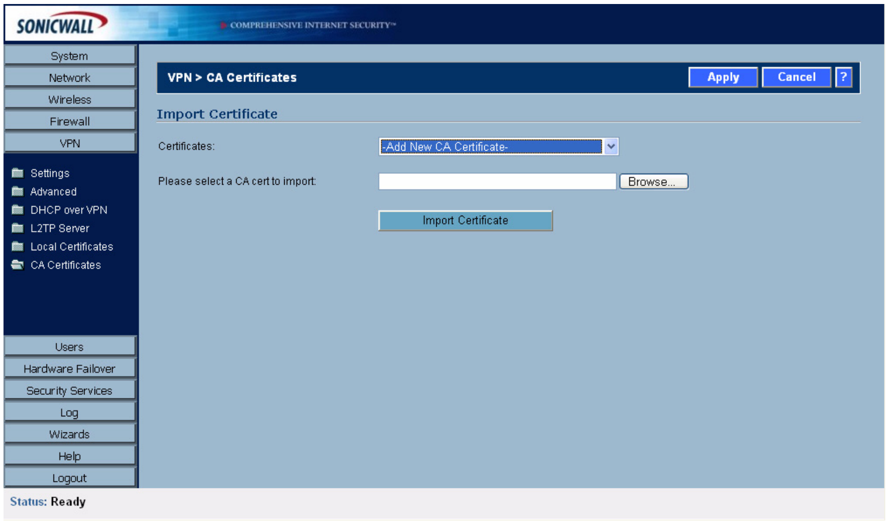
A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

SonicWALL security appliances support third party certificates from the following two vendors of Certificate Authority Certificates:

- VeriSign
- Entrust

Implementing Certificates for VPN Policies

To implement the use of certificates for VPN policies, you must locate a source for a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the SonicWALL security appliance to validate your Local Certificates. You import the valid CA certificate into the SonicWALL security appliance using the **VPN>CA Certificates** page.

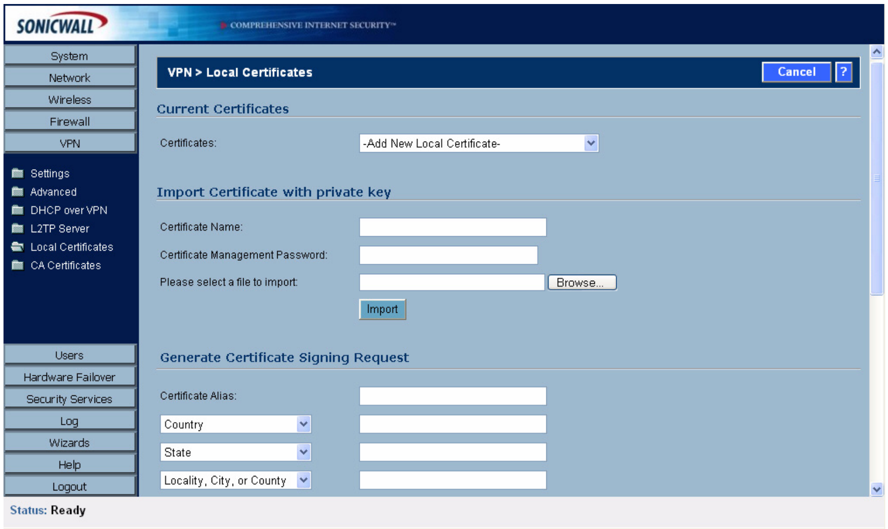

SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
VPN > CA Certificates
Apply
Cancel
?
Import Certificate
Browse...
Import Certificate

Certificates: -Add New CA Certificate-

Please select a CA cert to import:

Status: Ready

Once you import the valid CA certificate, you can use it to validate your local certificates you add in the **VPN>Local Certificates** page.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
VPN > Local Certificates
Cancel
?
Current Certificates
Import Certificate with private key
Browse...
Import
Generate Certificate Signing Request

Certificates: -Add New Local Certificate-

Certificate Name:

Certificate Management Password:

Please select a file to import:

Certificate Alias:

Country

State

Locality, City, or County

Status: Ready

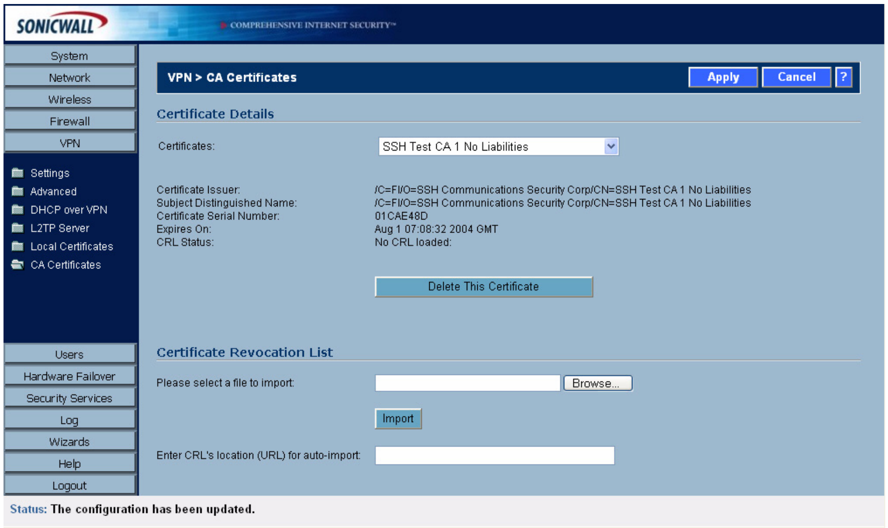
Importing CA Certificates into the SonicWALL Security Appliance

After your CA service has validated your **CA Certificate**, you can import it into the SonicWALL security appliance and use it to validate **Local Certificates** for VPN Security Associations.

Import your **CA Certificate** into the SonicWALL security appliance, follow these steps:

1. Select **Add New CA Certificate** from the **Certificates** menu.
2. Click **Browse**, then locate the PKCS#7 (*.p7b) or DER (*.der) or *.cer encoded file sent by the CA service. Click **Open** to set the directory path to the certificate.

3 Click **Import Certificate** to import the certificate into the SonicWALL security appliance. Once it is imported, you can view the **Certificate Details**.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
VPN > CA Certificates
Apply
Cancel
?
Delete This Certificate
Browse...
Import

Certificate Details

Certificates: SSH Test CA 1 No Liabilities

Certificate Issuer: /C=FI/O=SSH Communications Security Corp/CN=SSH Test CA 1 No Liabilities
Subject Distinguished Name: /C=FI/O=SSH Communications Security Corp/CN=SSH Test CA 1 No Liabilities
Certificate Serial Number: 01CAE48D
Expires On: Aug 1 07:08:32 2004 GMT
CRL Status: No CRL loaded:

Certificate Revocation List

Please select a file to import:

Enter CRL's location (URL) for auto-import:

Status: The configuration has been updated.

Certificate Details

The **Certificate Details** section lists the following information:

- Certificate Issuer
- Subject Distinguished Name
- Certificate Serial Number
- Expires On
- CRL Status

The **Certificate Issuer**, **Certificate Serial Number**, and the **Expiration Date** are generated by the CA service. The information is used when a **Generate Certificate Signing Request** is created and sent to your CA service for validation.

Delete This Certificate

To delete the certificate, click **Delete This Certificate**. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

Certificate Revocation List (CRL)

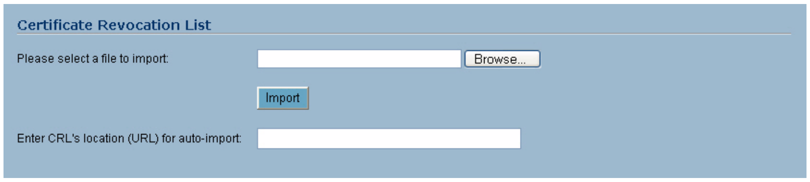
A **Certificate Revocation List (CRL)** is a way to check the validity of an existing certificate. A certificate may be invalid for several reasons:

- It is no longer needed.
- A certificate was stolen or compromised.
- A new certificate was issued that takes precedence over the old certificate.

If a certificate is invalid, the CA may publish the certificate on a **Certificate Revocation List** at a given interval, or on an online server in a X.509 v3 database using Online Certificate Status Protocol (OCSP). Consult your CA provider for specific details on locating a CRL file or URL.

✓ **Tip:** *The SonicWALL security appliance supports obtaining the CRL via HTTP or manually downloading the list.*

You can import the CRL by manually downloading the CRL and then importing it into the SonicWALL security appliance. You can also enter the URL location of the CRL by entering the address in the **Enter CRL's location (URL) for auto-import** field. The CRL is downloaded automatically at intervals determined by the CA service. Certificates are checked against the CRL by the SonicWALL security appliance for validity when they are used.


Certificate Revocation List
Please select a file to import:
Browse...
Import
Enter CRL's location (URL) for auto-import:

Importing a CRL List

To import a CRL list, follow these steps:

1. Click **Browse** for **Please select a file to import**.
2. Locate the PKCS#12 (*.p12) or Micorosft (*.pfx) encoded file.
3. Click **Open** to set the directory path to the certificate.
4. Click **Import** to import the certificate into the SonicWALL security appliance.

Automatic CRL Update

To enable automatic CRL updates to the SonicWALL security appliance, type the URL of the CRL server for your CA service in the **Enter CRL's location (URL) for auto-import**, then click Apply.

VPN > Local Certificates

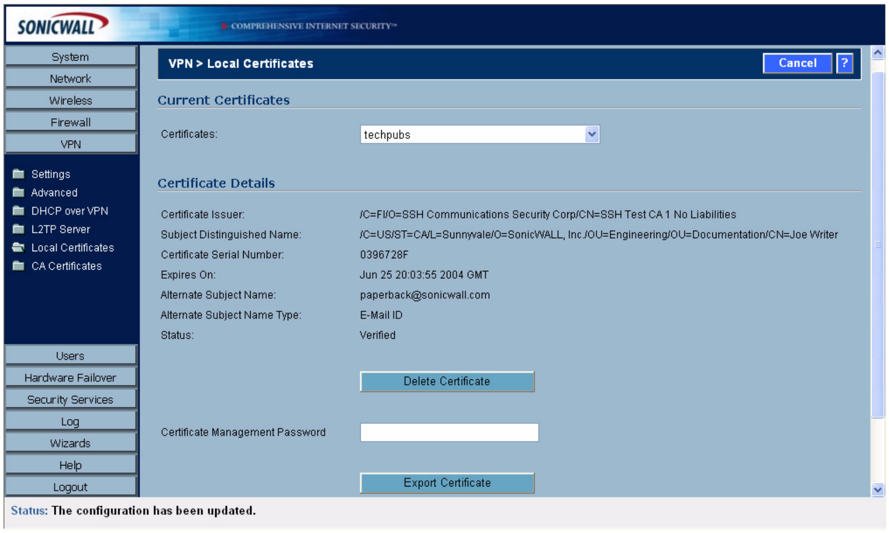
After a certificate is signed by the CA and returned to you, you can import the certificate into the SonicWALL security appliance to be used as a **Local Certificate** for a VPN Security Association.

Importing Certificate with Private Key

Use the following steps to import the certificate into the SonicWALL security appliance:

1. In the **Import Certificate with private key** section of the **Local Certificates** page, type the name of the certificate in the **Certificate Name** field.
2. Type password for the certificate in the **Certificate Management Password** field. This password was created when you exported your signed certificate.
3. Use **Browse** to locate the certificate file.
4. Click **Import**, and the certificate appears in the list of **Current Certificates**.

5 To view details about the certificate, select it from the Certificates menu in the **Current Certificates** section.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Settings
Advanced
DHCP over VPN
L2TP Server
Local Certificates
CA Certificates
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Cancel
?
Delete Certificate
Export Certificate

VPN > Local Certificates

Current Certificates

Certificates: techpubs

Certificate Details

Certificate Issuer: /C=FI/O=SSH Communications Security Corp/CN=SSH Test CA 1 No Liabilities
Subject Distinguished Name: /C=US/ST=CA/L=Sunnyvale/O=SonicWALL, Inc./OU=Engineering/OU=Documentation/CN=Joe Writer
Certificate Serial Number: 0396728F
Expires On: Jun 25 20:03:55 2004 GMT
Alternate Subject Name: paperback@sonicwall.com
Alternate Subject Name Type: E-Mail ID
Status: Verified

Certificate Management Password

Status: The configuration has been updated.

Certificate Details

To view details about the certificate, select the certificate from the **Certificates** menu in the **Current Certificates** section. The Certificate Details section lists the following information about the certificate:

- Certificate Issuer
- Subject Distinguished Name
- Certificate Serial Number
- Expiration On
- Alternate Subject Name
- Alternate Subject Name Type
- Status

Delete This Certificate

To delete the certificate, click **Delete This Certificate**. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

Generating a Certificate Signing Request

To generate a local certificate for use with a VPN policy, follow these steps:

✓ **Tip:** *You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.*

1 Select **Add New Local Certificate** from the **Certificates** menu.

2 In the **Generate Certificate Signing Request** section, enter an alias name for the certificate in the **Certificate Alias** field.

3 Select the Request field type from the menu, then enter information for the certificate in the Request fields. As you enter information in the Request fields, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.

You can also attach an optional **Subject Alternative Name** to the certificate such as the **Domain Name** or **E-mail Address**.

4 The **Subject Key** type is preset as an **RSA** algorithm. RSA is a public key cryptographic algorithm used for encrypting data.

5 Select a Subject Key size from the **Subject Key Size** menu.

Note: *Not all key sizes are supported by a Certificate Authority, therefore you should check with your CA for support key sizes.*

6 Click **Generate** to create a certificate file. Once the **Certificate Signing Request** is generated, a message describing the result is displayed.

7 Click **Export** to download the file to your computer, then click **Save** to save it to a directory on your computer.

You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.

PART

7

Users

:

CHAPTER 34

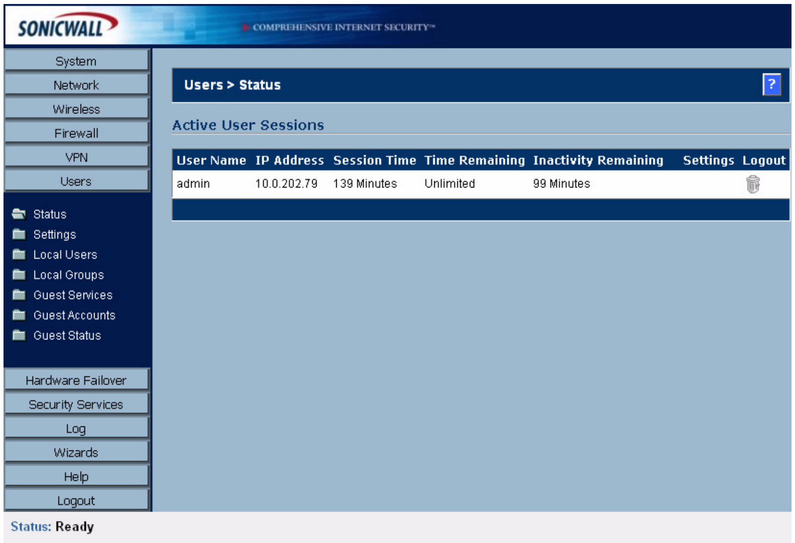
Managing User Status and Authentication Settings

SonicWALL security appliances provide a mechanism for user level authentication that gives users access to the LAN from remote locations on the Internet as well as a means to bypass content filtering. Also, you can permit only authenticated users to access VPN tunnels and send data across the encrypted connection.

User level authentication can performed using a local user database, RADIUS, or a combination of the two applications. The local database on the SonicWALL can support up to 1000 users. If you have more than 1000 users, you must use RADIUS for authentication

Users>Status

The **Users>Status** page displays **Active User Sessions** on the SonicWALL. The table lists **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, and **Logout**. To logout a user, click the Trashcan icon next to the user's entry.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Status
Settings
Local Users
Local Groups
Guest Services
Guest Accounts
Guest Status
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Users > Status
?

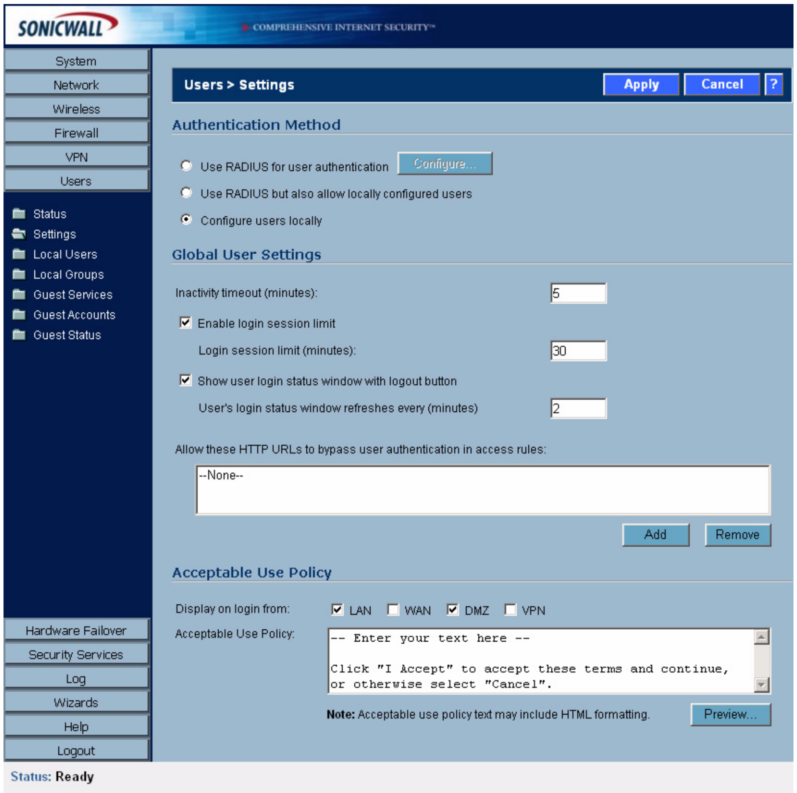
Active User Sessions

User Name	IP Address	Session Time	Time Remaining	Inactivity Remaining	Settings	Logout
admin	10.0.202.79	139 Minutes	Unlimited	99 Minutes		🗑

Status: Ready

User>Settings

On this page, you can configure the authentication method required, global user settings, and an acceptable user policy that is displayed to users when logging onto your network.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
VPN
Users
Status
Settings
Local Users
Local Groups
Guest Services
Guest Accounts
Guest Status
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Users > Settings
Apply
Cancel
?
Configure...
Add
Remove
Preview...

Authentication Method

○ Use RADIUS for user authentication

○ Use RADIUS but also allow locally configured users

● Configure users locally

Global User Settings

Inactivity timeout (minutes): 5

☑ Enable login session limit

Login session limit (minutes): 30

☑ Show user login status window with logout button

User's login status window refreshes every (minutes) 2

Allow these HTTP URLs to bypass user authentication in access rules:

--None--

Acceptable Use Policy

Display on login from: ☑ LAN ☐ WAN ☑ DMZ ☐ VPN

Acceptable Use Policy:

```
-- Enter your text here --

Click "I Accept" to accept these terms and continue,
or otherwise select "Cancel".
```

Note: Acceptable use policy text may include HTML formatting.

Status: Ready

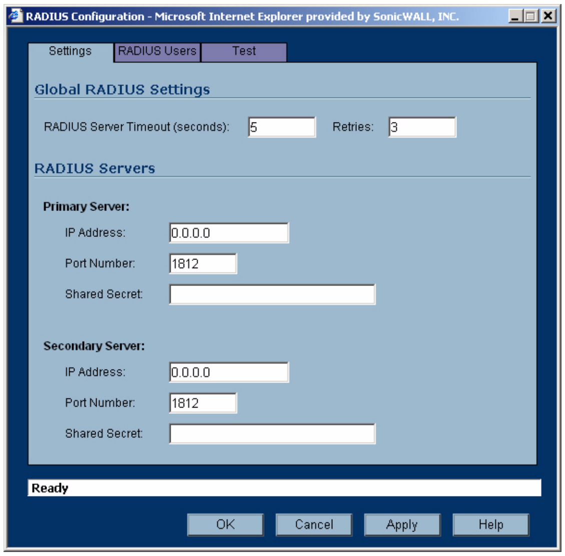
Authentication Method

- Select **Use RADIUS for user authentication** if you have more than 1,000 users or want to add an extra layer of security for authenticating the user to the SonicWALL. If you select Use RADIUS for user authentication, users must log into the SonicWALL using HTTPS in order to encrypt the password sent to the SonicWALL. If a user attempts to log into the SonicWALL using HTTP, the browser is automatically redirected to HTTPS.
- Select **Use RADIUS but also allow locally configured users** if you want to use both RADIUS and the SonicWALL local user database for authentication.
- Select **Configure users locally** to configure users in the local database using the **Users>Local Users** and **Users>Local Groups** pages.

Configuring RADIUS Authentication

If you selected **Use RADIUS for user authentication** or **Use RADIUS but also allow locally configured users**, the **Configure** button becomes available.

1. Click **Configure** to set up your RADIUS server settings on the SonicWALL. The **RADIUS Configuration** window is displayed.


RADIUS Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
RADIUS Users
Test
OK
Cancel
Apply
Help

Global RADIUS Settings

RADIUS Server Timeout (seconds): 5
Retries: 3

RADIUS Servers

Primary Server:
IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Secondary Server:
IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Ready

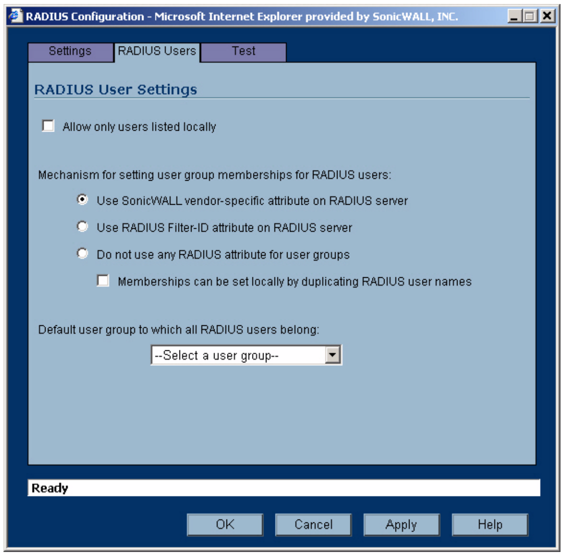
2. Define the **RADIUS Server Timeout in Seconds**. The allowable range is 1-60 seconds with a default value of 5.
3. Define the number of times the SonicWALL attempts to contact the RADIUS server in the **Retries** field. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, however 3 RADIUS server retries is recommended.

RADIUS Servers

1. Specify the settings of the primary RADIUS server in the RADIUS servers section. An optional secondary RADIUS server can be defined if a backup RADIUS server exists on the network.
2. Type the IP address of the RADIUS server in the **IP Address** field.
3. Type the **Port Number** for the RADIUS server.
4. Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.
5. If there is a secondary RADIUS server, type the appropriate information in the **Secondary Server** section.
6. Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.

RADIUS Users

Click the **RADIUS Users** tab.


RADIUS Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
RADIUS Users
Test
OK
Cancel
Apply
Help

RADIUS User Settings

☐ Allow only users listed locally

Mechanism for setting user group memberships for RADIUS users:

● Use SonicWALL vendor-specific attribute on RADIUS server

○ Use RADIUS Filter-ID attribute on RADIUS server

○ Do not use any RADIUS attribute for user groups

☐ Memberships can be set locally by duplicating RADIUS user names

Default user group to which all RADIUS users belong: --Select a user group--

Ready

RADIUS Users Settings

Select **Allow only users listed locally** if only the users listed in the SonicWALL database are authenticated using RADIUS.

Select the mechanism used for setting user group memberships for RADIUS users from the following list:

- **Use SonicWALL vendor-specific attribute on RADIUS server**: select to apply specific attributes from the RADIUS server.
- **Use RADIUS Filter-ID attribute on RADIUS server**
- **Do not use any RADIUS attributes for user groups**

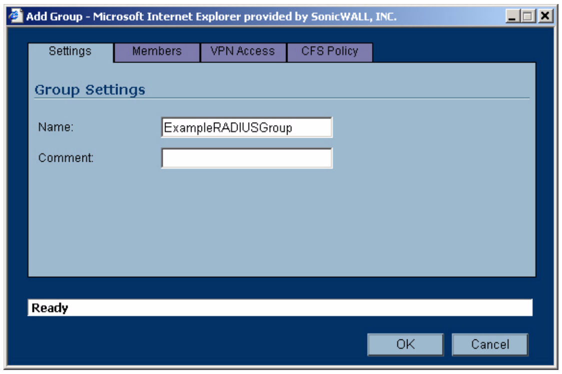
For a shortcut for managing RADIUS user groups, check **Memberships can be set locally by duplicating RADIUS user names**. When you create users with the same name locally on the security appliance and manage their group memberships, the memberships in the RADIUS database will automatically change to mirror your local changes.

If you have previously configured User Groups on the SonicWALL, select the group from the **Default user group to which all RADIUS user belong** menu.

You can create a new group by choosing **Create a new user group...** from the list:

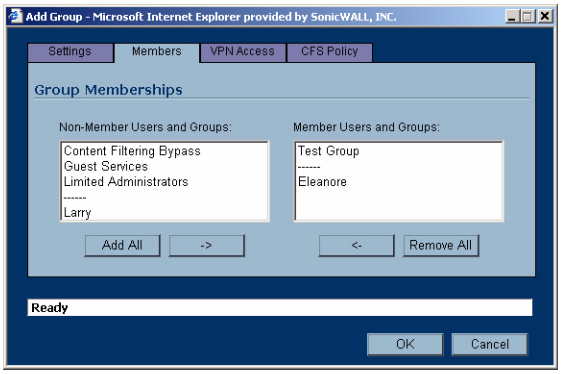
1. Select **Create a new user group...** The Add Group window displays.

2 In the **Settings** tab, enter a name for the group. You may enter a descriptive comment as well.


Add Group - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Members
VPN Access
CFS Policy
Group Settings
Ready
OK
Cancel

Name: ExampleRADIUSGroup
Comment:

3 In the **Members** tab, select the members of the group. Select the users or groups you want to add in the left column and click the **->** button. Click **Add All** to add all users and groups.


Add Group - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Members
VPN Access
CFS Policy
Group Memberships
Add All
->
<-
Remove All
Ready
OK
Cancel

Non-Member Users and Groups:
Content Filtering Bypass
Guest Services
Limited Administrators

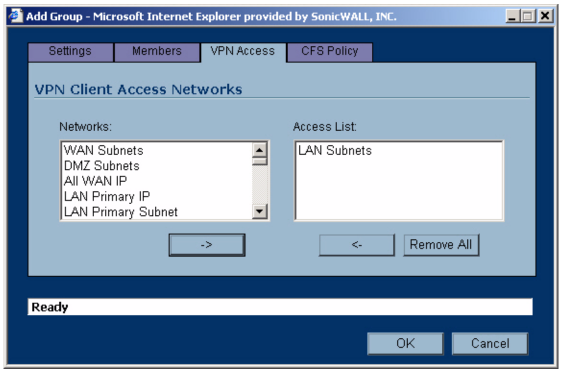
Larry

Member Users and Groups:
Test Group

Eleanore

Note: *You can add any group as a member of another group except **Everybody** and **All RADIUS Users**. Be aware of the membership of the groups you add as members of another group.*

4 In the **VPN Access** tab, select the network resources this group will have VPN Access to by default.


Add Group - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Members
VPN Access
CFS Policy
VPN Client Access Networks
->
<-
Remove All
Ready
OK
Cancel

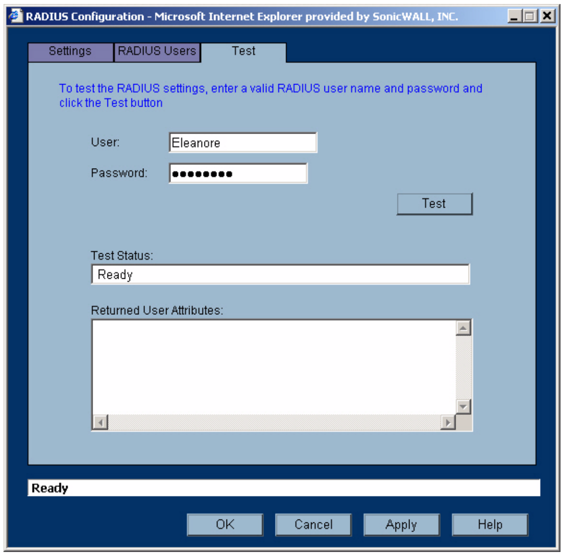
Networks:
WAN Subnets
DMZ Subnets
All WAN IP
LAN Primary IP
LAN Primary Subnet

Access List:
LAN Subnets

5 If you have Content Filtering Service (CFS) on your security appliance, you can configure the content filtering policy for this group in the **CFS Policy** tab. See **Chapter 39, Configuring SonicWALL Content Filter** for instructions on registering for and managing the SonicWALL Content Filtering Service.

RADIUS Client Test

You can test your RADIUS Client user name and password by typing in a valid user name in the **User** field, and the password in the **Password** field.


RADIUS Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
RADIUS Users
Test
Test
OK
Cancel
Apply
Help

To test the RADIUS settings, enter a valid RADIUS user name and password and click the Test button

User: Eleanore

Password: ••••••••

Test Status: Ready

Returned User Attributes:

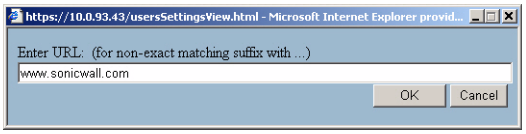
Ready

If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**. Once the SonicWALL has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to type a User Name and Password into a dialogue box.

Global User Settings

The settings listed below apply to all users when authenticated through the SonicWALL.

- **Inactivity timeout (minutes)**: users can be logged out of the SonicWALL after a preconfigured inactivity time. Enter the number of minutes in this field.
- **Enable login session limit**: you can limit the time a user is logged into the SonicWALL by selecting the check box and typing the amount of time, in minutes, in the **Login session limit (minutes)** field. The default value is **30** minutes.
- **User's login status page refreshes every (minutes)**: defines the time between user login status page refreshes. The default is **2** minutes.
- **Allow these HTTP URLs to bypass users authentication access rules**: Define a list of URLs users can connect to without authenticating. To add a URL to the list:
  a Click **Add** below the URL list.
  b In the Enter URL window, enter the top level URL you are adding, for example, `www.sonicwall.com`. All sub directories of that URL are included, such as `www.sonicwall.com/services/documentation.html`. Click on **OK** to add the URL to the list.


https://10.0.93.43/usersSettingsView.html - Microsoft Internet Explorer provid...
OK
Cancel

Enter URL: (for non-exact matching suffix with ...)

www.sonicwall.com

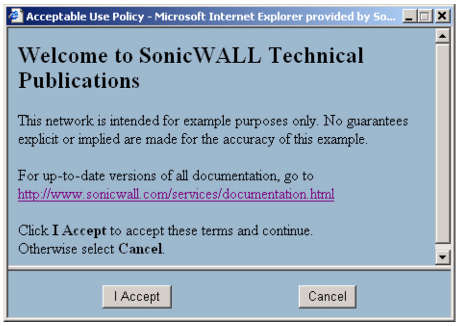
Acceptable Use Policy

An acceptable use policy (AUP) is a policy users must agree to follow in order to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through the SonicWALL.

LAN and **DMZ/OPT** are selected automatically from the **Display on login** from section. **WAN** and **VPN** are also available.

In the **Acceptable Use Policy** field, enter the text of your policy. Click **Apply** to update the configuration.

Click the **Preview** button to display your AUP message as it will appear for the user.


Acceptable Use Policy - Microsoft Internet Explorer provided by So...

Welcome to SonicWALL Technical Publications

This network is intended for example purposes only. No guarantees explicit or implied are made for the accuracy of this example.

For up-to-date versions of all documentation, go to http://www.sonicwall.com/services/documentation.html

Click **I Accept** to accept these terms and continue.
Otherwise select **Cancel**.

✓ **Tip:** *Acceptable Use Policies can use HTML formatting in the body of the message. The text of the message in the example image above is:*

```
<h2>Welcome to SonicWALL Technical Publications </h2> This network is intended
for example purposes only. No guarantees explicit or implied are made for the
accuracy of this example.

For up-to-date versions of all documentation, go to <a href="http://
www.sonicwall.com/services/documentation.html">http://www.sonicwall.com/
services/documentation.html</a>

Click <b>I Accept</b> to accept these terms and continue. <br>Otherwise select
<b>Cancel</b>.
```

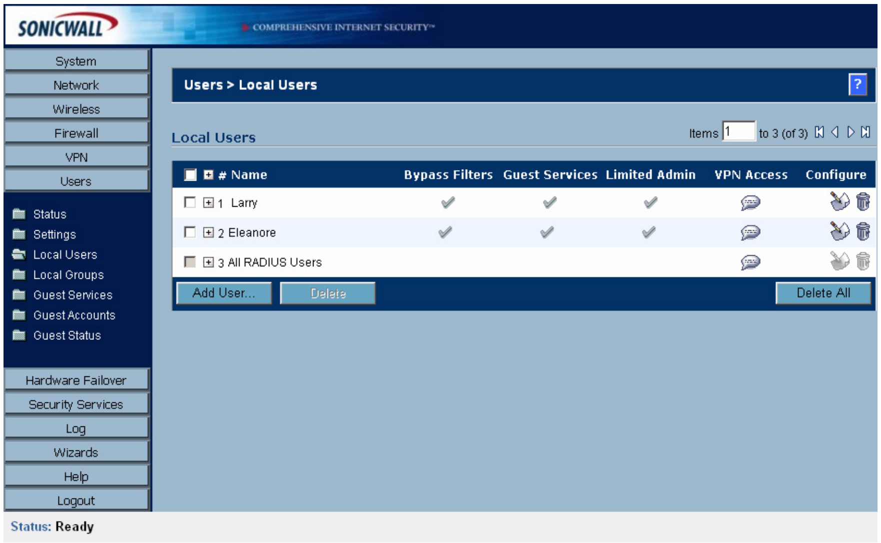
CHAPTER 35

Managing Local Users and Local Groups

User > Local Users

Local Users are users stored and managed on the security appliance’s local database.

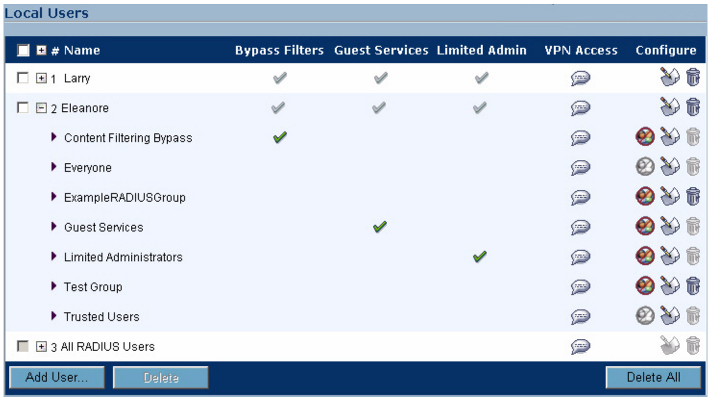
In the he Users > Local Users page, you can view and manage all local users, add new local users, and edit existing local users.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Status
Settings
Local Users
Local Groups
Guest Services
Guest Accounts
Guest Status
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Users > Local Users
?
Local Users
Items 1 to 3 (of 3)
Add User...
Delete
Delete All
Status: Ready

☐ # Name	Bypass Filters	Guest Services	Limited Admin	VPN Access	Configure
☐ 1 Larry	✓	✓	✓		
☐ 2 Eleanore	✓	✓	✓		
☐ 3 All RADIUS Users					

Viewing Local Users

You can view all the groups a user belongs to on the Users > Local Users page. Click on the expand icon ⊞ next to a user to view the group memberships for that user.


Local Users
Add User...
Delete
Delete All

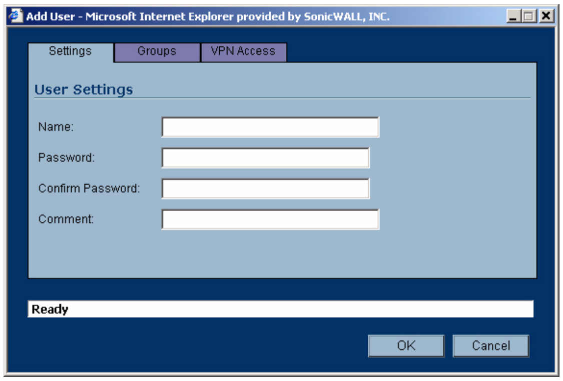
# Name	Bypass Filters	Guest Services	Limited Admin	VPN Access	Configure
☐ ⊞ 1 Larry	✓	✓	✓		
☐ ⊟ 2 Eleanore	✓	✓	✓		
Content Filtering Bypass	✓				
Everyone					
ExampleRADIUSGroup					
Guest Services		✓			
Limited Administrators			✓		
Test Group					
Trusted Users					
☐ ⊞ 3 All RADIUS Users					

The three columns to the right of the user's name list the privileges the user has. In the expanded view, it displays which group the user gets each privilege from.

- Hover the mouse pointer over the comment icon in the VPN Access column to view the network resources the user has VPN access to.
- In the expanded view, click the remove icon under Configure to remove the user from a group.
- Click the edit icon under Configure to edit the user.
- Click the delete icon under Configure to delete the user or group in that row.

Adding Local Users

To add local users to the security appliance's internal database. Click **Add User** to display the **Add User** configuration window. Follow the steps below to add users locally.

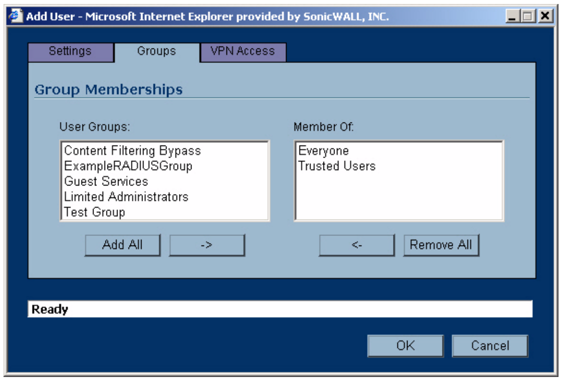

Add User - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Groups
VPN Access
User Settings
Name:
Password:
Confirm Password:
Comment:
Ready
OK
Cancel

Settings

1. Create a user name and type it in the **User Name** field.
2. Create a password for the user and type it in the **Password** field. Passwords are case-sensitive and should consist of a combination of letters and numbers rather than names of family, friends, or pets.
3. Confirm the password by retyping it in the **Confirm Password** field.

Groups

To add the user to a User Group, select one or more groups, and click ->. The user then becomes a member of the selected groups. To remove a group, select the group from the Member of column, and click <-.


Add User - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Groups
VPN Access
Add All
->
<-
Remove All
OK
Cancel

Group Memberships

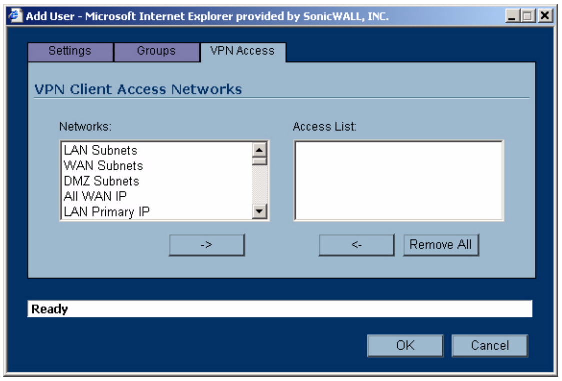
User Groups:
Content Filtering Bypass
ExampleRADIUSGroup
Guest Services
Limited Administrators
Test Group

Member Of:
Everyone
Trusted Users

Ready

VPN Access

To allow users to access networks using a VPN tunnel, select the network from the **Networks** list and click -> to move it to the **Access List.**


Add User - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Groups
VPN Access
->
<-
Remove All
OK
Cancel

VPN Client Access Networks

Networks:
LAN Subnets
WAN Subnets
DMZ Subnets
All WAN IP
LAN Primary IP

Access List:

Ready

To remove a network from the **Access List**, select the network and click <-. Click **OK** to complete the user configuration.

Editing Local Users

You can edit local users from the Users > Local Users screen. To edit a local user, In the list of users, click the edit icon in same line as the user you are editing.

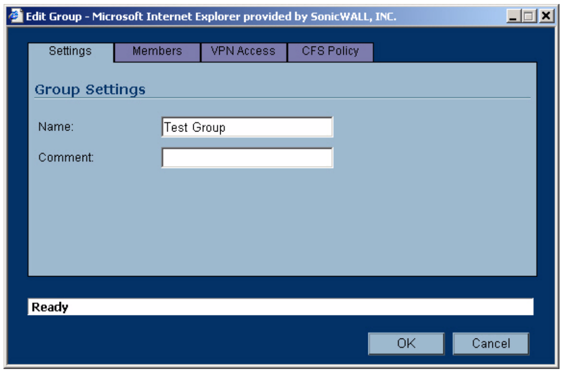
Configure the Settings, Groups, and VPN Access exactly as when adding a new user.

Guest Services

Click the Guest Services tab to enable guest service for this user.

Users>Local Groups

Local groups are displayed in the **Local Groups** table. The table lists **Name**, **Bypass Filters**, **Limited Admin**, **VPN Access**, and **Configure**. A default group, **Everyone**, is listed in the first row of the table. Click the Notepad icon in the **Configure** column to review or change the settings for **Everyone**.


Edit Group - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Members
VPN Access
CFS Policy
Group Settings
OK
Cancel

Name: Test Group

Comment:

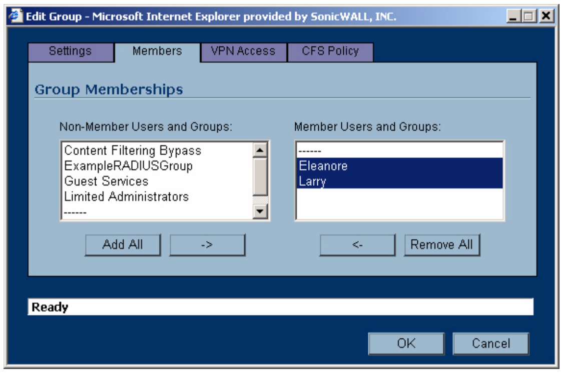
Ready

Creating a Local Group

1. Click the **Add Group** button to display the **Add Group** window.
2. Create a user name and type it in the **User Name** field.
3. Select any of the following options from the Group Settings section:

- **Bypass Filters** - select **Bypass Filters** if the user has unlimited access to the Internet from the LAN, bypassing Web, News, Java, and ActiveX blocking.
- **Limited Management Capabilities** - By enabling this check box, the user has limited local management access to the SonicWALL Management interface. The access is limited to the following pages:
    - **General** - Status, Network, Time
    - **Log** - View Log, Log Settings, Log Reports
    - **Tools** - Restart, Diagnostics minus Tech Support Report

4. To add non-Members Users and Groups, click the **Members** tab. Select the non-member user or group from the **Non-Members Users and Groups** list and click ->.


Edit Group - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Members
VPN Access
CFS Policy
Group Memberships
Add All
->
<-
Remove All
OK
Cancel

Non-Member Users and Groups:
Content Filtering Bypass
ExampleRADIUSGroup
Guest Services
Limited Administrators

Member Users and Groups:

Eleanore
Larry

Ready

5. To allow users in this group to access networks using a VPN tunnel, click the **VPN Access** tab, select the network from the **Networks** list and click -> to move it to the **Access List.**
6. To enforce a custom Content Filtering Service policy for this group, click on the **CFS Policy** tab. Select the CFS policy from the **Policy** menu.

Note: *You create custom Content Filtering Service policies in the Security Services>Content Filter page.*

7. Click **OK**.

CHAPTER

36

Managing Guest Services and Guest Accounts

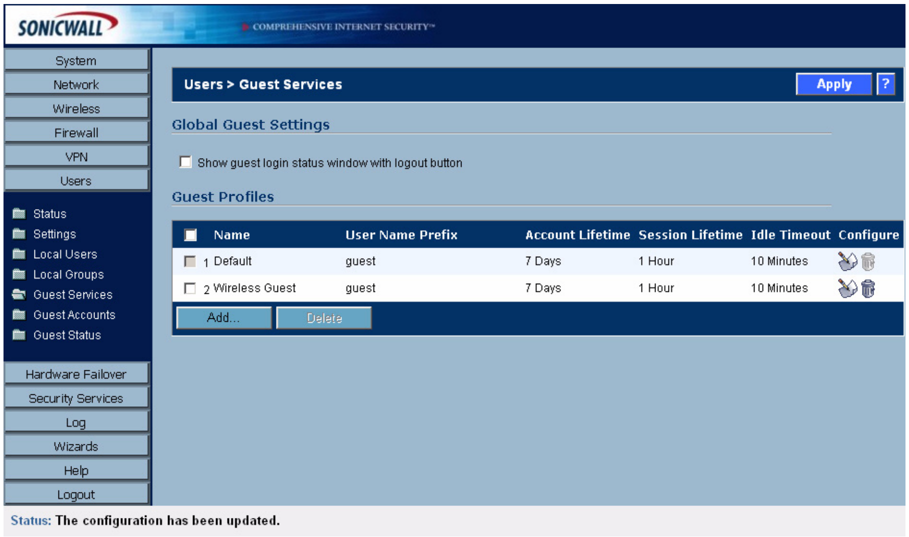
Guest accounts are temporary accounts set up for users to log into your network.

You can create these accounts manually, as needed or generate them in batches. SonicOS includes profiles you can configure in advance to automate configuring guest accounts when you generate them.

Guest accounts are typically limited to a pre-determined life-span. After their life span, by default, the accounts are removed.

Users > Guest Services

Guest Services determine the limits and configuration of the guest accounts. The Users > Guest services page displays a list of Guest Profiles. Guest profiles determine the configuration of guest accounts when they are generated. In the Users > Guest Services page, you can add, delete, and configure Guest Profiles. In addition, you can determine if all users who log in to the security appliance see a user login window that displays the amount of time remaining in their current login session.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Status
Settings
Local Users
Local Groups
Guest Services
Guest Accounts
Guest Status
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Users > Guest Services
Apply
?
Add...
Delete

Global Guest Settings

☐ Show guest login status window with logout button

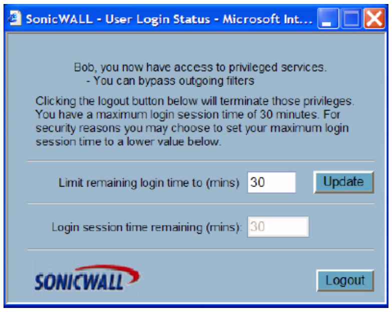
Guest Profiles

☐	Name	User Name Prefix	Account Lifetime	Session Lifetime	Idle Timeout	Configure
☐ 1	Default	guest	7 Days	1 Hour	10 Minutes	
☐ 2	Wireless Guest	guest	7 Days	1 Hour	10 Minutes	

Status: The configuration has been updated.

Global Guest Settings

Check **Show guest login status window with logout button** to display a user login window on the users's workstation whenever the user is logged in. Users must keep this window open during their login session. The window displays the time remaining in their current session. Users can log out but clicking the **Logout** button in the login status window.



Bob, you now have access to privileged services.
- You can bypass outgoing filters

Clicking the logout button below will terminate those privileges. You have a maximum login session time of 30 minutes. For security reasons you may choose to set your maximum login session time to a lower value below.

Limit remaining login time to (mins) 30

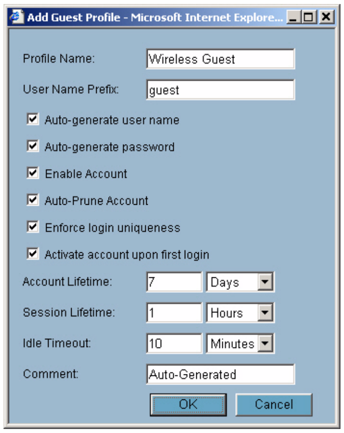
Login session time remaining (mins): 30

Guest Profiles

The Guest Profiles list shows the profiles you have created and enables you to add, edit, and delete profiles.

To add a profile:

1 Click **Add** below the Guest Profile list to display the Add Guest Profile window.



Profile Name: Wireless Guest
User Name Prefix: guest
☑ Auto-generate user name
☑ Auto-generate password
☑ Enable Account
☑ Auto-Prune Account
☑ Enforce login uniqueness
☑ Activate account upon first login
Account Lifetime: 7 Days
Session Lifetime: 1 Hours
Idle Timeout: 10 Minutes
Comment: Auto-Generated

2 In the Add Guest Profile window, configure:

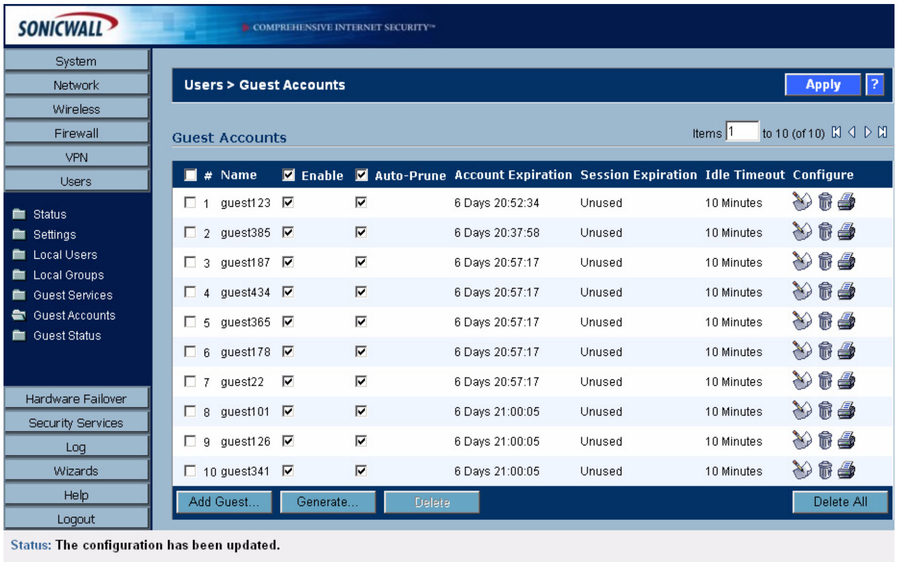
- **Profile Name**: Enter the name of the profile.
- **User Name Prefix**: Enter the first part of every user account name generated from this profile.
- **Auto-generate user name**: Check this to allow guest accounts generated from this profile to have an automatically generated user name. The user name is usually the prefix plus a two- or three-digit number.
- **Auto-generate password**: Check this to allow guest accounts generated from this profile to have an automatically generated password. The generated password is an eight-character unique alphabetic string.
- **Enable Account**: Check this for all guest accounts generated from this profile to be enabled upon creation.
- **Auto-Prune Account**: Check this to have the account removed from the database after its lifetime expires.

- **Enforce login uniqueness**: Check this to allow only a single instance of an account to be used at any one time. By default, this feature is enabled when creating a new guest account. If you want to allow multiple users to login with a single account, disable this enforcement by clearing the Enforce login uniqueness checkbox.
- **Activate account upon first login**: Check this for the account to remain inactive until the user logs in and activates the account.
- **Account Lifetime**: This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.
- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**
- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.
- **Comment**: Any text can be entered as a comment in the **Comment** field.

3 Click **OK** to add the profile.

Users > Guest Accounts

The Users > Guest Accounts page lists the guest services accounts on the security appliance. In the guest services accounts, you can enable or disable individual accounts, groups of accounts, or all accounts, you can set the Auto-Prune feature for accounts, and you can add, edit, delete, and print accounts.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
VPN
Users
Status
Settings
Local Users
Local Groups
Guest Services
Guest Accounts
Guest Status
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Users > Guest Accounts
Apply
?
Guest Accounts
Items 1 to 10 (of 10)
Add Guest...
Generate...
Delete
Delete All

☐	#	Name	☑ Enable	☑ Auto-Prune	Account Expiration	Session Expiration	Idle Timeout	Configure
☐	1	guest123	☑	☑	6 Days 20:52:34	Unused	10 Minutes	
☐	2	guest385	☑	☑	6 Days 20:37:58	Unused	10 Minutes	
☐	3	guest187	☑	☑	6 Days 20:57:17	Unused	10 Minutes	
☐	4	guest434	☑	☑	6 Days 20:57:17	Unused	10 Minutes	
☐	5	guest365	☑	☑	6 Days 20:57:17	Unused	10 Minutes	
☐	6	guest178	☑	☑	6 Days 20:57:17	Unused	10 Minutes	
☐	7	guest22	☑	☑	6 Days 20:57:17	Unused	10 Minutes	
☐	8	guest101	☑	☑	6 Days 21:00:05	Unused	10 Minutes	
☐	9	guest126	☑	☑	6 Days 21:00:05	Unused	10 Minutes	
☐	10	guest341	☑	☑	6 Days 21:00:05	Unused	10 Minutes	

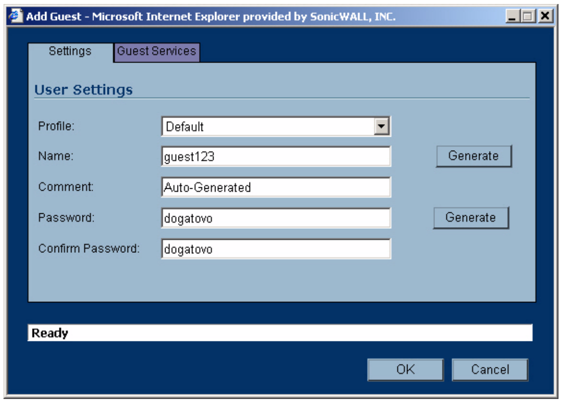
Status: The configuration has been updated.

Adding Guest Accounts

You can add guest accounts individually or generate multiple guest accounts automatically.

To Add an Individual Account:

1 Under the list of accounts, click **Add Guest**.


Add Guest - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Guest Services
User Settings
Generate
Generate
Ready
OK
Cancel

Profile: Default
Name: guest123
Comment: Auto-Generated
Password: dogatovo
Confirm Password: dogatovo

2 In the **Settings** tab of the Add Guest Account window configure:

- **Profile**: Select the Guest Profile to generate this account from.
- **Name**: Enter a name for the account or click **Generate**. The generated name is the prefix in the profile and a random two or three digit number.
- **Comment**: Enter a descriptive comment.
- **Password**: Enter the user account password or click **Generate**. The generated password is a random string of eight alphabetic characters.
- **Confirm** Password: If you did not generate the password, re-enter it.

Note: *Make a note of the password. Otherwise you will have to reset it.*

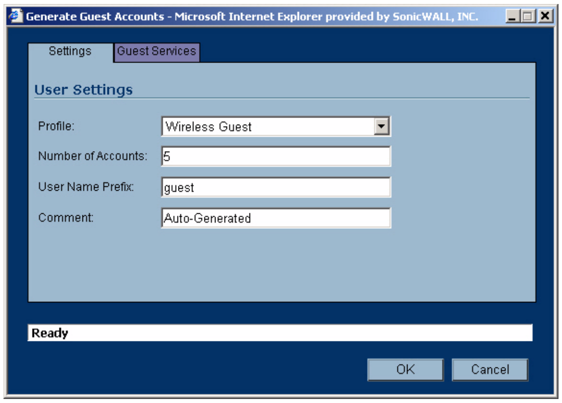
3 In the **Guest Services** tab, configure:

- **Enable Guest Services Privilege**: Check this for the account to be enabled upon creation.
- **Enforce login uniqueness**: Check this to allow only one instance of this account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration**: Check this to have the account removed from the database after its lifetime expires.
- **Account Lifetime**: This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.
- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

4 Click **OK** to generate the account.

To Generate Multiple Accounts

1 Under the list of accounts, click **Generate**.


Generate Guest Accounts - Microsoft Internet Explorer provided by SonicWALL, INC.
Settings
Guest Services
Ready
OK
Cancel

User Settings

Profile: Wireless Guest
Number of Accounts: 5
User Name Prefix: guest
Comment: Auto-Generated

2 In the **Settings** tab of the Generate Guest Accounts window configure:

- **Profile**: Select the Guest Profile to generate the accounts from.Number of Accounts:
- **Number of Accounts**: Enter the number of accounts to generate.
- **User Name Prefix**: Enter the prefix from which account names are generated. For example, if you enter **Guest** the generated accounts will have names like “Guest 123” and “Guest 234”.
- **Comment**: Enter a descriptive comment.

3 In the **Guest Services** tab, configure:

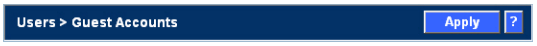
- **Enable Guest Services Privilege**: Check this for the accounts to be enabled upon creation.
- **Enforce login uniqueness**: Check this to allow only one instance of each generated account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration**: Check this to have the account removed from the database after its lifetime expires.
- **Account Lifetime**: This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.
- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

4 Click **OK** to generate the accounts.

Enabling Guest Accounts

You can enable or disable any number of accounts at one time. To enable one or more guest accounts:

1 Check the box in the **Enable** column next to the name of the account you want to enable. Check the **Enable** box in the table heading to enable all accounts on the page.
2 Click on **Apply** in the top right corner of the page.



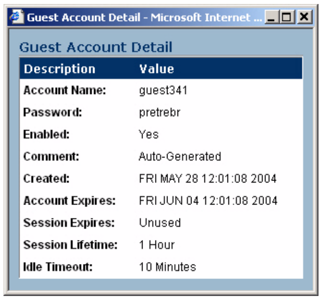
Enabling Auto-prune for Guest Accounts

You can enable or disable auto-prune for any number of accounts at one time. When auto-prune is enabled, the account is deleted after it expires. To enable auto-prune:

1 Check the box in the **Auto-Prune** column next to the name of the account. Check the **Auto-Prune** box in the table heading to enable it on all accounts on the page.
2 Click on **Apply** in the top right corner of the page.

Printing Account Details.

You can print a summary of a guest account. Click the print icon to launch a summary account report page and send that page to an active printer.

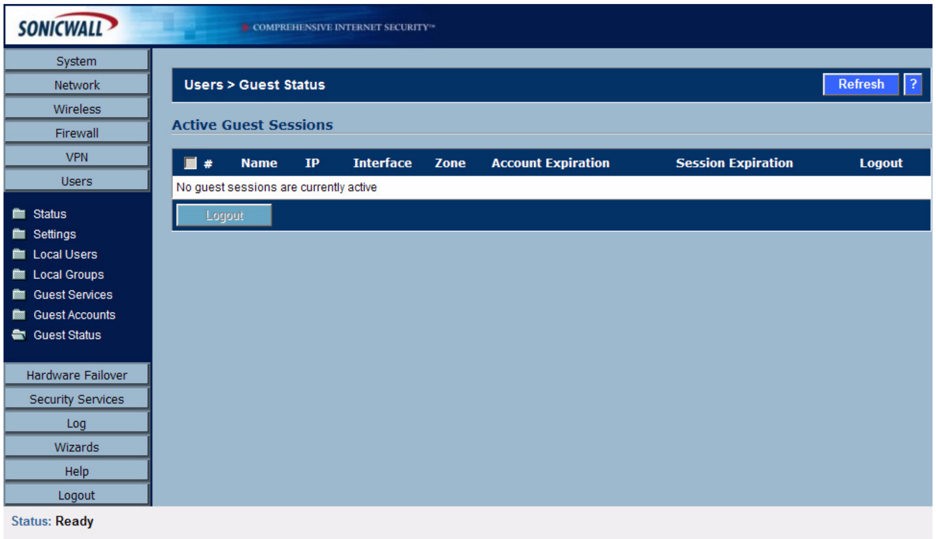


Guest Account Detail

Description	Value
Account Name:	guest341
Password:	pretrebr
Enabled:	Yes
Comment:	Auto-Generated
Created:	FRI MAY 28 12:01:08 2004
Account Expires:	FRI JUN 04 12:01:08 2004
Session Expires:	Unused
Session Lifetime:	1 Hour
Idle Timeout:	10 Minutes

Users > Guest Status

The Guest Status page reports on all the guest accounts currently logged in to the security appliance.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Status
Settings
Local Users
Local Groups
Guest Services
Guest Accounts
Guest Status
Hardware Failover
Security Services
Log
Wizards
Help
Logout
Users > Guest Status
Refresh
?
Active Guest Sessions
# Name IP Interface Zone Account Expiration Session Expiration Logout
Logout

No guest sessions are currently active

Status: Ready

The page lists:

- **Name**: The name of the guest account
- **IP**: The IP address the guest user is connecting to.
- **Interface**: The interface on the security appliance through which the user account is connecting to the appliance. For example, If the guest account is a wireless user connecting through a SonicWALL SonicPoint, and all SonicPoints are connecting to the X3 port on the appliance, which is configured as a Wireless Zone, the **Interface** column will list **X3**.
- **Zone**: The Zone on the security appliance that the guest user is connecting to. For example, a wireless user might be connecting to the **WLAN** zone.
- **Account Expiration**: The date, hour, or minute when the account expires.
- **Session Expiration**: The time when the current session expires.
- **Logout**: Click the Logout icon to log the guest user off of the security appliance.

Click **Refresh** in the top right of the page at any time to update the information in the list.

Logging Accounts off the Appliance

As administrator, you can log users off the security appliance:

- To log an individual user out, click the Logout icon in the **Logout** column for that user.
- To log multiple users out, click the checkbox in the first column to select individual users, or check the checkbox next to the **#** in the table heading to select all the guest users listed on the page. Then click **Logout** below the list.

8

Hardware Failover

:

CHAPTER

37

Setting Up Hardware Failover

Hardware Failover > Settings

Hardware Failover allows two identical SonicWALL PRO Series security appliances running SonicOS Enhanced to be configured to provide a reliable, continuous connection to the public Internet. In the event of the failure of the Primary SonicWALL, the Backup SonicWALL takes over to secure a reliable connection between the protected network and the Internet.

How Hardware Failover Works

Hardware Failover requires one SonicWALL device configured as the Primary SonicWALL, and an identical SonicWALL device configured as the Backup SonicWALL. During normal operation, the Primary SonicWALL is in an Active state and the Backup SonicWALL in an Idle state. When a failure on the Primary SonicWALL occurs, the Backup SonicWALL transitions to Active mode and assumes the configuration and role of Primary. The failover applies to loss of functionality or network-layer connectivity on the Primary SonicWALL.

SonicWALL security appliance configuration is performed on only the Primary SonicWALL, with no need to perform any configuration on the Backup SonicWALL. The Backup SonicWALL contains a real-time mirrored configuration of the Primary SonicWALL via a dedicated Ethernet link. If the firmware configuration becomes corrupted on the Primary SonicWALL, the Backup SonicWALL automatically refreshes the Primary SonicWALL with the last-known-good copy of the configuration preferences.

The Primary and Backup SonicWALL appliances have unique MAC addresses and communicate via the X3 interface on the PRO2040 series, and via the X5 interface on the PRO3060/4060/5060 series. The dedicated HF interface link transmits all synchronization information from the Primary SonicWALL to the Backup SonicWALL.

There are two types of synchronization: incremental and complete. If the timestamps are in sync and a change is made on the Active unit, an incremental sync is pushed to the Idle unit. If the timestamps are out of sync and the Idle unit is available, a complete sync is pushed to the Idle unit. When incremental synchronization fails, a complete synchronization is automatically attempted.

Crash Detection

The Hardware Failover feature has a thorough self-diagnostic mechanism for both the Primary and Backup SonicWALL security appliances. The failover to the Backup SonicWALL occurs when critical services are affected, physical (or logical) link detection is detected on monitored interfaces, or when the SonicWALL loses power.

The self-checking mechanism is managed by software diagnostics, which check the complete system integrity of the SonicWALL device. The diagnostics check internal system status, system process status, and both internal and external network connectivity. For example, if a network topology has three levels, then diagnostics are performed on the router/switch/hub connectivity on the first, second, and third level. There is a weighting mechanism on both sides to decide which side has better connectivity, used to avoid potential failover looping.

Critical internal system processes such as NAT, VPN, and DHCP (among others) are checked in real time. The failing service is isolated as early as possible, and the failover mechanism repairs it automatically.

Before Configuring Hardware Failover

Before attempting to configure two SonicWALL appliances as a **Hardware Failover** pair, check the following requirements:

- Hardware Failover is only supported on the SonicWALL PRO 2040, PRO 3060, PRO 4060 and PRO 5060 security appliances running SonicOS Enhanced. It is not supported in any version of SonicOS Standard, or on any SonicWALL TZ 170 series product running the version of SonicOS Enhanced
- The Primary and Backup SonicWALL security appliances must be same hardware model – mixing and matching SonicWALLs of different hardware types is not currently supported.
- The Hardware Failover feature requires three unique LAN IP addresses to operate – the first IP address is used as a virtual gateway IP address, the second is used as the unique LAN IP address for the Primary device, and the third is used as the unique LAN IP address for the Backup device. You have at least one (1) valid, static IP address available from your Internet Service Provider (ISP). Two (2) valid, static IP addresses are required to remotely manage both the primary SonicWALL and the backup SonicWALL.

▲ **Alert:** *SonicWALL Hardware Failover does not support dynamic IP address assignment from your ISP.*

- Each SonicWALL security appliance in the **Hardware Failover** pair must have the same firmware version installed.
- SonicWALL Security Services licenses are not shared between Primary and Backup SonicWALL devices -- the Backup SonicWALL must have separate licenses. Each SonicWALL security appliance in the **Hardware Failover** pair must have the same SonicWALL Security Services enabled. If the Backup SonicWALL security appliance does not have the same upgrades and subscriptions enabled, these functions are not supported in the event of a failure of the Primary SonicWALL appliance.
- All SonicWALL ports being used must be connected together with a hub or switch. If each SonicWALL has a unique WAN IP Address for remote management, the WAN IP Addresses must be in the same subnet.

✓ **Tip:** *The two SonicWALLs in the Hardware Failover pair send "heartbeats" on their X5 Interfaces*—on the PRO3060/4060/5060 series—*as a dedicated-HF link. However, the PRO2040 series uses the X3 Interface as the dedicated-HF link.*

- If using new single WAN IP method, please note that the Backup device, when in offline 'Idle' mode, will not be able to use NTP to synchronize its internal clock, nor will it be able to contact the backend services licensing servers. It is also unable to perform device registration with the backend licensing servers.
- Hardware Failover can be used with dual WAN ports, but only if both WAN interfaces use static IP addressing; the current firmware does not support either WAN interface using dynamic IP addressing.

- Once Hardware Failover has been configured and activated, upon first preferences synchronization, the Backup SonicWALL security appliance automatically reboots in order to load the mirrored preferences – this is normal behavior.
- At present, the monitor feature utilizes ICMP pings on designated probe targets, and can only be used on interfaces that have been assigned unique IP addresses (at present, LAN and WAN only).
- The Primary and Backup SonicWALL security appliance's unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use the virtual LAN IP address as their gateway.
- The Primary and Backup SonicWALL devices are currently only capable of performing active/ passive Hardware Failover – active/active failover is not supported at present.
- Session state is not currently synchronized between the Primary and Backup SonicWALL security appliances. If a failover occurs, any session that had been active at the time of failover needs to be renegotiated.
- If shifting a previously assigned interface to act as the Secondary WAN interface, be sure to remove any custom NAT policies that were associated with that interface before configuring it.
- It's strongly recommended that Primary and Backup SonicWALL security appliances run the exact same version of firmware; system instability may result if firmware versions are out of sync.
- Successful Hardware Failover synchronization is not logged, only failures.
- If you are connecting the Primary and Backup device to an Ethernet switch running the spanning-tree protocol, please be aware that it may be necessary to adjust the link activation time on the switch port that the SonicWALL interfaces connect to. As an example, it would be necessary to activate spantree portfast on a Cisco Catalyst-series switch, for each port connecting to the SonicWALL's interfaces.
- If you will not be using the unique WAN IP address feature, make sure each entry field is set to '0.0.0.0' – the SonicWALL will report an error if the field is left blank.

Hardware Failover Terminology

- **Primary** - Describes the principal hardware unit itself. The Primary identifier is a manual designation, and is not subject to conditional changes. Under normal operating conditions, the Primary hardware unit operates in an Active role.
- **Backup** - Describes the subordinate hardware unit itself. The Backup identifier is a relational designation, and is assumed by a unit when paired with a Primary unit. Under normal operating conditions, the Backup unit operates in an Idle mode. Upon failure of the Primary unit, the Backup unit will assume the Active role.
- **Active** - Describes the operative condition of a hardware unit. The Active identifier is a logical role that can be assumed by either a Primary or Backup hardware unit.
- **Idle** - Describes the passive condition of a hardware unit. The Idle identifier is a logical role that can be assumed by either a Primary or Backup hardware unit. The Idle unit assumes the Active role in the event of determinable failure of the Active unit.
- **Failover** - The actual process in which the Idle unit assumes the Active role following a qualified failure of the Active unit. Qualification of failure is achieved by various configurable physical and logical monitoring facilities described throughout the Task List section.
- **Preempt** - Applies to a post-failover condition in which the Primary unit has failed, and the Backup unit has assumed the Active role. Enabling Preempt will cause the Primary unit to seize the Active role from the Backup after the Primary has been restored to a verified operational state.

Intial Hardware Failover Setup

Before you begin the configuration of Hardware Failover on the Primary SonicWALL security appliance, perform the following intial setup procedures.

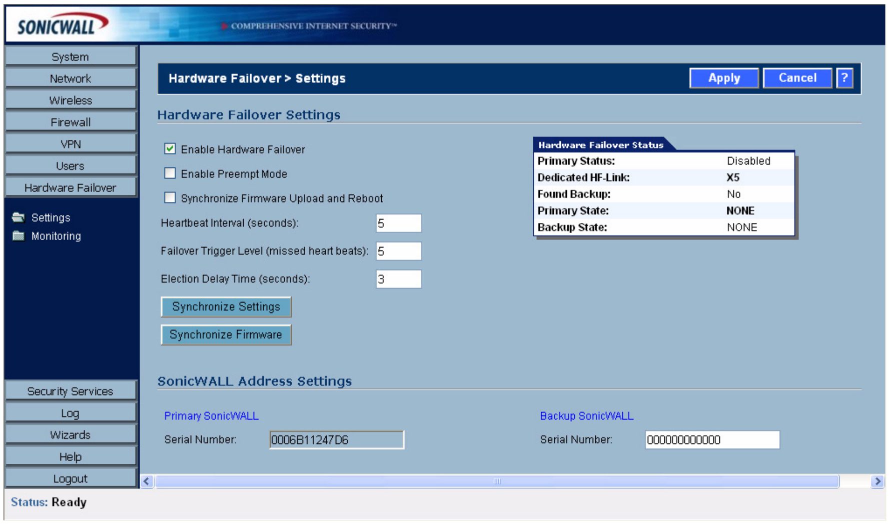
- On the back of the Backup SonicWALL security appliance, local the serial number and write the number down. You need to enter this number in the **Hardware Failover>Settings** page.
- Check to make sure the Primary SonicWALL and Backup SonicWALL security appliances are registered, running the same SonicOS Enhanced versions, and running the same SonicWALL Security Security services.
- Make sure Primary SonicWALL and Backup SonicWALL security appliance's LAN, WAN, and other interfaces are properly configured for seamless failover.
- Connect the X5 ports on the Primary SonicWALL and Backup SonicWALL appliances with a CAT6-rated crossover cable. The Primary and Backup SonicWALL security appliances must have a dedicated connection between each other using the X3 (PRO2040) or X5 (PRO3060/4060/5060) interface. SonicWALL recommends cross-connecting the two together using a CAT5/6 crossover Ethernet cable, but a connection using a dedicated 100Mbps hub/switch is also acceptable.
- Power up the Primary SonicWALL security appliance, and then power on the Backup SonicWALL security appliance.
- Do not make any configuration to the Primary's X3 (PRO 2040) or X5 (PRO 3060/4060/5060) interface; the Hardware Failover programming in an upcoming step takes care of this issue. When done, disconnect the workstation.

Configuring Hardware Failover

The first task in setting up hardware failover after intial setup is configuring the **Hardware Failover>Settings** page on the Primary SonicWALL security appliance. Once you configure hardware failover on the Primary SonicWALL security appliance, you push out the settings to the Backup SonicWALL security appliance.

To configure Hardware Failover on the Primary SonicWALL, perform the following steps:

1 Select the **Hardware Failover>Settings** page on the Primary SonicWALL.



Hardware Failover > Settings

Hardware Failover Settings

☑ Enable Hardware Failover
☐ Enable Preempt Mode
☐ Synchronize Firmware Upload and Reboot
Heartbeat Interval (seconds): 5
Failover Trigger Level (missed heart beats): 5
Election Delay Time (seconds): 3

Hardware Failover Status	
Primary Status:	Disabled
Dedicated HF-Link:	**X5**
Found Backup:	No
Primary State:	**NONE**
Backup State:	NONE

SonicWALL Address Settings

Primary SonicWALL
Serial Number: 0006B11247D6

Backup SonicWALL
Serial Number: 000000000000

Status: **Ready**

2 In the **Serial Number** field under **Backup SonicWALL**, enter the Backup SonicWALLs Serial number (this can be found on the back of the device).

3 Leave the **Heartbeat Interval (seconds)**, **Failover Trigger Level (missed heart beats)** and **Election Delay Time (seconds)** timers to their default settings. These timers can be tuned later as necessary for your specific network environment. A description of these timers and their effects are covered in an upcoming section.

4 Check the **Enable Hardware Failover** and the **Enable Preempt Mode** checkboxes. If everything is configured and cabled correctly, the Primary SonicWALL automatically contacts the Backup SonicWALL over the dedicated link and configures all necessary settings. The Backup SonicWALL then reboots with its new settings and come back online in Idle mode.

5 Click the **Apply** button to save the changes.

Sychronize Settings

Once you've configured the hardware failover setting on the Primary SonicWALL security appliance, click the **Synchronize Settings** button. You should see a **HA Peer Firewall has been updated** message at the bottom of the Management Interface page. Also note that the Management Interface displays **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

To verify that Primary and Backup SonicWALL security appliances are functioning correctly, wait a few minutes, then power off the Primary SonicWALL device. The Backup SonicWALL security appliance should quickly take over.

From your Management Workstation, test connectivity through the Backup SonicWALL by accessing a site on the public Internet – note that the Backup SonicWALL, when active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

Log into the Backup SonicWALL's unique LAN IP address. If this SonicWALL security appliance has not been registered at mySonicWALL.com, register it. The Management Interface should now display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

Now, power the Primary SonicWALL back on, wait a few minutes, then log back into the Management Interface. The Management GUI should again display **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure everything is working correctly.

Forcing Transitions

In some cases, it may be necessary to force a transition from one active SonicWALL to another – for example, to force the primary SonicWALL to become active again after a failure when **Preempt Mode** has not been enabled, or to force the backup SonicWALL to become active in order to do preventive maintenance on the primary SonicWALL.

To force such a transition, it is necessary to interrupt the heartbeat from the currently active SonicWALL. This may be accomplished by disconnecting the active SonicWALL's LAN port, by shutting off power on the currently active unit, or by restarting it from the Web Management Interface. In all of these cases, heartbeats from the active SonicWALL are interrupted, which forces the currently **Idle** unit to become **Active**.

To restart the active SonicWALL, log into the primary SonicWALL LAN IP Address and click **Tools** on the left side of the browser window and then click **Restart** at the top of the window.

Click **Restart SonicWALL**, then **Yes** to confirm the restart. Once the active SonicWALL restarts, the other SonicWALL in the **Hardware Failover** pair takes over operation.

Alert: *If the Preempt Mode checkbox has been checked for the primary SonicWALL, the primary unit takes over operation from the backup unit after the restart is complete.*

Adjusting Hardware Failover Settings

On the **Hardware Failover>Settings** page, there are three user-configurable timers that can be adjusted to suit your network's needs:

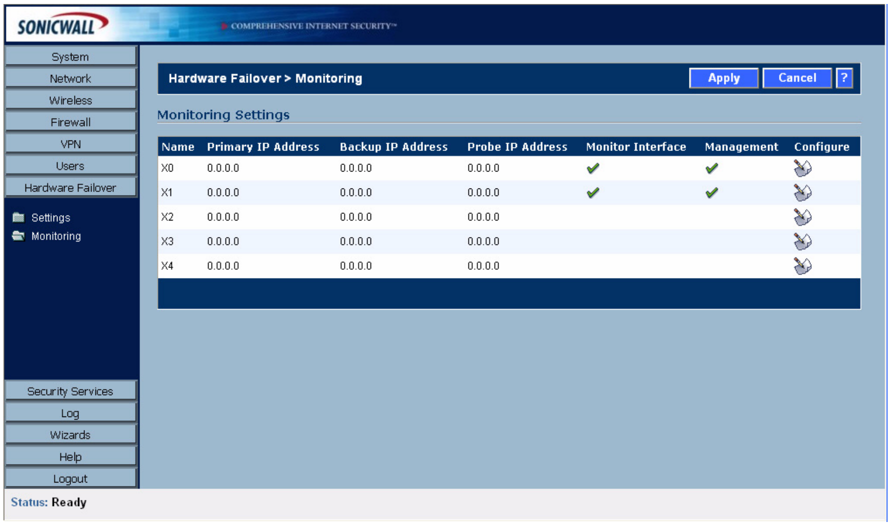
- **Heartbeat Interval (seconds)** – This timer is the length of time between status checks. By default this timer is set to 5 seconds; using a longer interval will result in the SonicWALL taking more time to detect when/if failures have occurred.
- **Failover Trigger Level (missed heart beats)** – This timer is the number of heartbeats the SonicWALL will miss before failing over. By default, this time is set to 5 missed heart beats.This timer is linked to the Heartbeat Interval timer – for example, if you set the Heartbeat Interval to 10 seconds, and the Failover Trigger Level timer to 5, it will be 50 seconds before the SonicWALL fails over.
- **Election Delay Time** – This timer can be used to specify an amount of time the SonicWALL will wait to consider an interface up and stable, and is useful when dealing with switch ports that have a spanning-tree delay set.

Sychronizing Firmware

Checking the **Sychronize Firmware Upload and Reboot** checkbox allows the Primary And Backup SonicWALL security appliances in Hardware Failover mode to have firmware uploaded on both devices at once, in staggered sequence to ensure security is always maintained. During the firmware upload and reboot, you are notified via a message dialog box that the firmware is loaded on the Backup SonicWALL security appliance, and then the Primary SonicWALL security appliance. You initiate this process by clicking on the **Synchronize Firmware** button.

Monitoring Links

On the **Hardware Failover>Monitoring** page, you can specify IP addresses that the SonicWALL security appliance performs an ICMP ping on to determine link viability.



Name	Primary IP Address	Backup IP Address	Probe IP Address	Monitor Interface	Management	Configure
X0	0.0.0.0	0.0.0.0	0.0.0.0	✓	✓	✎
X1	0.0.0.0	0.0.0.0	0.0.0.0	✓	✓	✎
X2	0.0.0.0	0.0.0.0	0.0.0.0			✎
X3	0.0.0.0	0.0.0.0	0.0.0.0			✎
X4	0.0.0.0	0.0.0.0	0.0.0.0			✎

When using logical monitors, the SonicWALL will ping the defined ‘Probe IP Address’ target from the Primary as well as the Backup SonicWALL. If both can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as the SonicWALLs will assume that the problem is with the target, and not the SonicWALLs. But, if one SonicWALL can ping the target but the other SonicWALL cannot, it will failover to the SonicWALL that can ping the target.

Hardware Failover Status

If failure of the primary SonicWALL occurs, the backup SonicWALL assumes the primary SonicWALL LAN and WAN IP Addresses. There are three primary methods to check the status of the High Availability pair: the Hardware Failover Status window, E-mail Alerts and View Log. These methods are described in the following sections.

- **Hardware Failover Status** - One method to determine which SonicWALL is active is to check the Hardware Failover Settings Status indicator on the Hardware Failover>Settings page. If the primary SonicWALL is active, the first line in the page indicates that the primary SonicWALL is currently Active. It is also possible to check the status of the backup SonicWALL by logging into the LAN IP Address of the backup SonicWALL. If the primary SonicWALL is operating normally, the status indicates that the backup SonicWALL is currently Idle. If the backup has taken over for the primary, the status indicates that the backup is currently Active. In the event of a failure in the primary SonicWALL, you can access the Management Interface of the backup SonicWALL at the primary SonicWALL LAN IP Address or at the backup SonicWALL LAN IP Address. When the primary SonicWALL restarts after a failure, it is accessible using the third IP address created during configuration. If preempt mode is enabled, the primary SonicWALL becomes the active firewall and the backup firewall returns to Idle status.

- **E-mail Alerts Indicating Status Change** - If you have configured the primary SonicWALL to send E-mail alerts, you receive alert e-mails when there is a change in the status of the Hardware Failover pair. For example, when the backup SonicWALL takes over for the primary after a failure, an e-mail alert is sent indicating that the backup has transitioned from Idle to Active. If the primary SonicWALL subsequently resumes operation after that failure, and Preempt Mode has been enabled, the primary SonicWALL takes over and another e-mail alert is sent to the administrator indicating that the primary has preempted the backup.
- **View Log** - The SonicWALL also maintains an event log that displays the Hardware Failover events in addition to other status messages and possible security threats. This log may be viewed with a browser using the SonicWALL Management Interface or it may be automatically sent to the administrator’s E-mail address. To view the SonicWALL log, click Log on the left side of the management interface.

PART

9

Security Services

:

CHAPTER

38

Managing Security Services

Security Services>Summary

SonicWALL, Inc. offers a variety of subscription-based Security Services and Upgrades to enhance the functionality of your SonicWALL security appliance to provide complete protection. You can activate and manage Security Services directly from the SonicWALL Management Interface or from mySonicWALL.com https://www.mySonicWALL.com.

Note: *For more information on SonicWALL Security Services and Upgrades, visit the SonicWALL Web site http://www.sonicwall.com.*

This chapter provides an overview of the SonicWALL Security Services listed under **Security Services** in the SonicWALL Management Interface. These subscription-based services include:

- SonicWALL Content Filtering Service
- SonicWALL Network Anti-Virus
- SonicWALL E-Mail Filter
- SonicWALL Intrusion Prevention Service

✓ **Tip:** *You can try FREE TRIAL of these services directly from the SonicWALL Management Interface.*

This chapter also explains how to configure the SonicWALL Restrict Web Features and Trusted Domains features on the **Security Services>Content Filtering** page that are included with SonicOS Enhanced.

Note: *For complete product documentation on any SonicWALL Security Service, go to the SonicWALL documentation site at www.sonicwall.com/services/documentation.*

mySonicWALL.com

mySonicWALL.com delivers a convenient, one-stop resource for registration, activation, and management of your SonicWALL products and services. Your mySonicWALL.com account provides a single profile to do the following:

- Register your SonicWALL security appliances
- Purchase/Activate SonicWALL Security Services and Upgrades
- Receive SonicWALL firmware and security service updates and alerts
- Manage (change or delete) your SonicWALL security services
- Access SonicWALL Technical Support

Creating a mySonicWALL.com account is easy and FREE. Simply complete an online registration form. Once your account is created, you can register SonicWALL security appliance and activate SonicWALL Security Services associated with the security appliance.

Your mySonicWALL.com account is accessible from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information. You can also access mySonicWALL.com license and registration services directly from the SonicWALL management interface for increased ease of use and simplified services activation.

✓ **Tip:** *For more information on mySonicWALL.com, access the online help available at https://www.mysonicwall.com.*

Note: *mySonicWALL.com registration information is not sold or shared with any other company.*

➲ **Cross Reference:** *If you don't have a mySonicWALL.com account, see Chapter 3 Viewing SonicWALL Security Appliance Status Information for instructions on setting up an account via the SonicWALL Management Interface.*

If Your SonicWALL is Not Registered

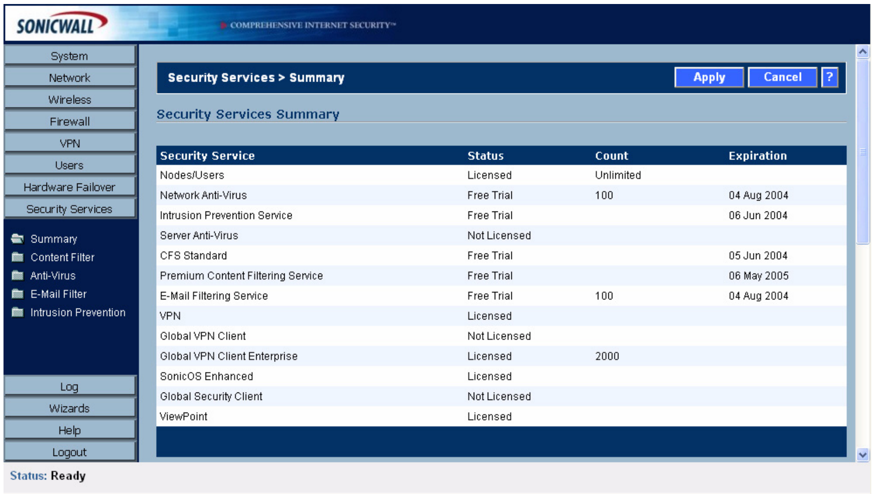
If your SonicWALL security appliance is not registered, the **Security Services>Summary** page does not include the **Services Summary** table. Your SonicWALL must be registered to display the **Services Summary** table.

You can register your SonicWALL via the Management Interface on the **System>Status** page. You must have a mySonicWALL.com account to register your SonicWALL via the Management Interface. You can create a mySonicWALL.com account from the Security **Services>Summary** page using the **Manage Licenses** button to display the **mySonicWALL.com Login** page.

➲ **Cross Reference:** *If your SonicWALL security appliance is not registered, see Chapter 3 Viewing SonicWALL Security Appliance Status Information for instructions on registering your SonicWALL via the SonicWALL Management Interface.*

Security Services Summary

A list of currently available services through mySonicWALL.com is displayed in the **Security Services Summary** table. Subscribed services are displayed with **Licensed** in the **Status** column. If the service is limited to a number of users, the number is displayed in the **Count** column. The service expiration date is displayed in the **Expiration** column.



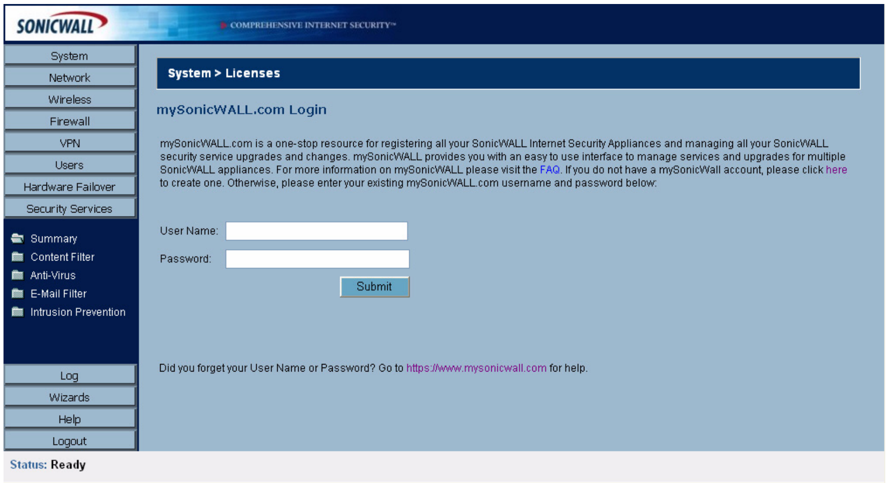
Security Services Summary

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
Network Anti-Virus	Free Trial	100	04 Aug 2004
Intrusion Prevention Service	Free Trial		06 Jun 2004
Server Anti-Virus	Not Licensed		
CFS Standard	Free Trial		05 Jun 2004
Premium Content Filtering Service	Free Trial		06 May 2005
E-Mail Filtering Service	Free Trial	100	04 Aug 2004
VPN	Licensed		
Global VPN Client	Not Licensed		
Global VPN Client Enterprise	Licensed	2000	
SonicOS Enhanced	Licensed		
Global Security Client	Not Licensed		
ViewPoint	Licensed		

Status: Ready

Manage Licenses

Clicking the **Manage Licenses** button displays the **mySonicWALL.com Login** page.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Summary
Content Filter
Anti-Virus
E-Mail Filter
Intrusion Prevention
Log
Wizards
Help
Logout
Submit
Status: Ready

System > Licenses

mySonicWALL.com Login

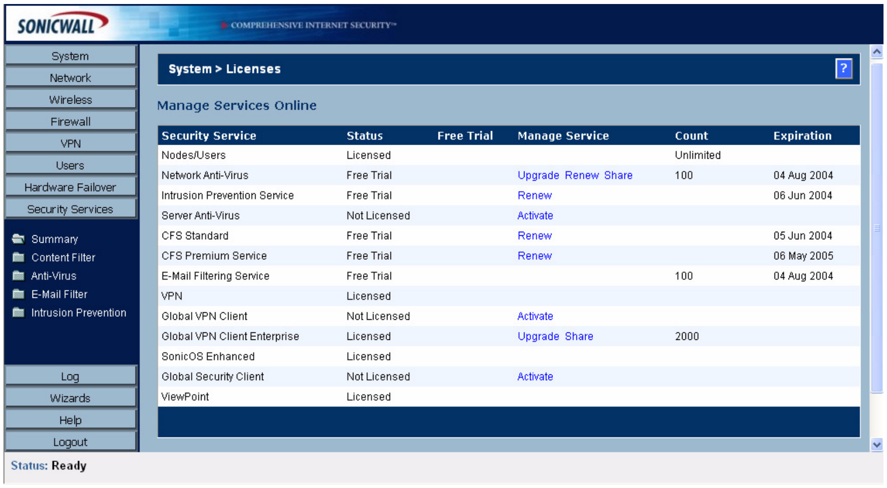
mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall account, please click here to create one. Otherwise, please enter your existing mySonicWALL.com username and password below:

User Name:

Password:

Did you forget your User Name or Password? Go to https://www.mysonicwall.com for help.

Enter your mySonicWALL.com username and password in the **User Name** and **Password** fields, and then click **Submit**. The **System>Licenses** page is displayed with the **Manage Services Online** table. The information in the **Manage Services Online** table is updated from your mySonicWALL.com account.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Summary
Content Filter
Anti-Virus
E-Mail Filter
Intrusion Prevention
Log
Wizards
Help
Logout
?
Status: Ready

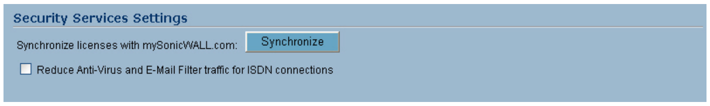
System > Licenses

Manage Services Online

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Free Trial		Upgrade Renew Share	100	04 Aug 2004
Intrusion Prevention Service	Free Trial		Renew		06 Jun 2004
Server Anti-Virus	Not Licensed		Activate		
CFS Standard	Free Trial		Renew		05 Jun 2004
CFS Premium Service	Free Trial		Renew		06 May 2005
E-Mail Filtering Service	Free Trial			100	04 Aug 2004
VPN	Licensed				
Global VPN Client	Not Licensed		Activate		
Global VPN Client Enterprise	Licensed		Upgrade Share	2000	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Licensed				

Note: *If you have activated SonicWALL Global Security Client on your SonicWALL, a* ***Policy Editor*** *button is displayed below the Manage Services Online table for configuring security policies. See the SonicWALL Global Security Client Administrator's Guide for instructions on configuring the Policy Editor.*

Security Services Settings


Synchronize

Security Services Settings

Synchronize licenses with mySonicWALL.com:

☐ Reduce Anti-Virus and E-Mail Filter traffic for ISDN connections

- **Synchronize** - Click **Synchronize** to update the licensing and subscription information on the SonicWALL from your mySonicWALL.com account.
- **Reduce Anti-Virus and E-mail Filter traffic for ISDN connections** - Selecting this feature enables the SonicWALL Anti-Virus to only check daily (every 24 hours) for updates and reduces the frequency of outbound traffic for users who do not have an "always on" Internet connection.

CHAPTER

39

Configuring SonicWALL Content Filter

Security Services>Content Filter

The **Security Services>Content Filter** page allows you to configure the SonicWALL Restrict Web Features and Trusted Domains settings, which are included with SonicOS Enhanced. You can activate and configure SonicWALL Content Filtering Service as well as two third-party Content Filtering products from the **Security Services>Content Filter** page.

SonicWALL Content Filtering Service

SonicWALL Content Filtering Service (CFS) enforces protection and productivity policies for businesses, schools and libraries to reduce legal and privacy risks while minimizing administration overhead. SonicWALL CFS utilizes a dynamic database of millions of URLs, IP addresses and domains to block objectionable, inappropriate or unproductive Web content. At the core of SonicWALL CFS is an innovative rating architecture that cross references all Web sites against the database at worldwide SonicWALL co-location facilities. A rating is returned to the SonicWALL security appliance and then compared to the content filtering policy established by the administrator. Almost instantaneously, the Web site request is either allowed through or a Web page is generated by the SonicWALL security appliance informing the user that the site has been blocked according to policy.

With SonicWALL CFS, network administrators have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. SonicWALL CFS automatically updates the filters, making maintenance substantially simpler and less time consuming.

SonicWALL CFS can also be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the SonicWALL security appliance, a customized message is displayed on the user's screen. SonicWALL security appliance can also be configured to log attempts to access sites on the SonicWALL Content Filtering Service database, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

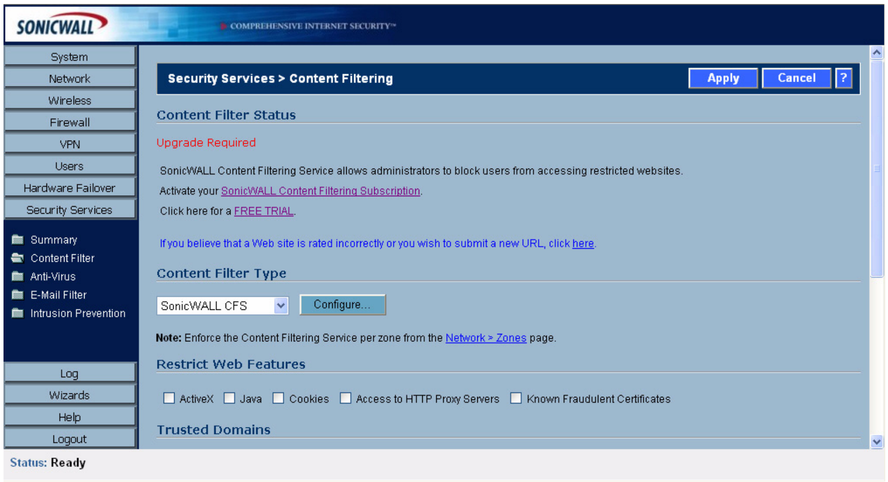
- **SonicWALL CFS Standard** blocks 12 categories of objectionable, inappropriate or unproductive Web content. SonicWALL CFS Standard runs on SonicOS Standard 2.0 (or higher).

- **SonicWALL CFS Premium** blocks 56 categories of objectionable, inappropriate or unproductive Web content. SonicWALL CFS Premium provides network administrators with greater control by automatically and transparently enforces acceptable use policies. It gives administrators the flexibility to enforce custom content filtering policies for groups of users on the network. For example, a school can create one policy for teachers and another for students. SonicWALL CFS Premium Productivity Edition and the SonicWALL CFS Premium Government/Education Edition run on SonicOS Standard 2.1 (or higher) as well as SonicOS Enhanced 2.0 (or higher).

Cross Reference: *For complete SonicWALL Content Filtering Service documentation, see the SonicWALL Content Filtering Service Administrator's Guide available on your Resource CD or online at http://www.sonicwall.com/services/documentation.html.*

Content Filter Status

If SonicWALL CFS is activated, the **Content Filter Status** section displays the status of the Content Filter Server, as well as the date and time that your subscription expires. The expiration date and time is displayed in Universal Time Code (UTC) format.



Security Services > Content Filtering

Content Filter Status

Upgrade Required

SonicWALL Content Filtering Service allows administrators to block users from accessing restricted websites.

Activate your SonicWALL Content Filtering Subscription.

Click here for a FREE TRIAL.

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.

Content Filter Type

SonicWALL CFS

Note: Enforce the Content Filtering Service per zone from the Network > Zones page.

Restrict Web Features

☐ ActiveX ☐ Java ☐ Cookies ☐ Access to HTTP Proxy Servers ☐ Known Fraudulent Certificates

Trusted Domains

Status: Ready

You can also access the **SonicWALL CFS URL Rating Review Request** form by clicking on the **here** link in **If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here**.

If SonicWALL CFS is not activated, you must activate it. If you do not have an Activation Key, you must purchase SonicWALL CFS from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada).

Activating SonicWALL CFS

If you have an Activation Key for your SonicWALL CFS subscription, follow these steps to activate SonicWALL CFS:

Alert: *You must have a mySonicWALL.com account and your SonicWALL security appliance must be registered to activate SonicWALL Network Anti-Virus.*

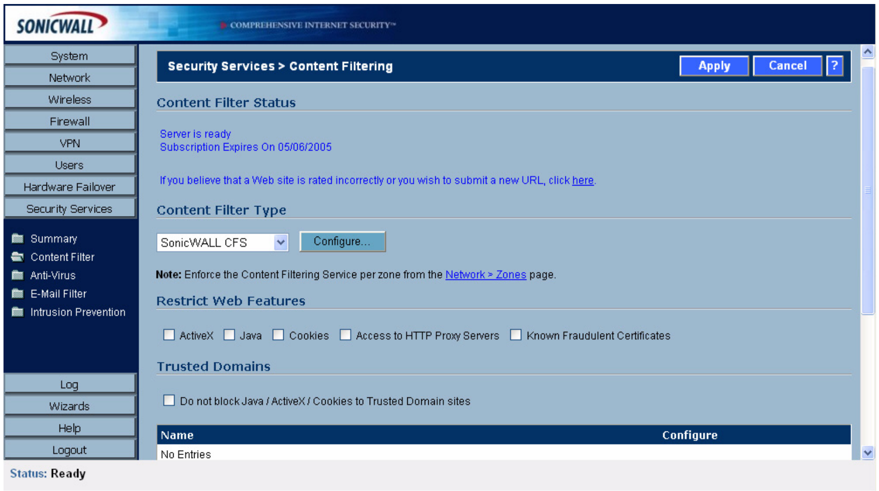
1. Click the **SonicWALL Content Filtering Subscription** link on the Security **Services>Content Filtering** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.

3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL CFS subscription is activated on your SonicWALL.
4. If you activated SonicWALL CFS at mySonicWALL.com, the SonicWALL CFS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services>Summary** page to update your SonicWALL.

Activating a SonicWALL CFS FREE TRIAL

You can try a FREE TRIAL of SonicWALL CFS by following these steps:

1. Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **FREE TRIAL** link.
3. Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL CFS trial subscription is activated on your SonicWALL.
4. Select **Security Services>Content Filter** to display the Content Filter page for configuring your SonicWALL Content Filtering Service settings.



Security Services > Content Filtering

Content Filter Status

Server is ready
Subscription Expires On 05/06/2005

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.

Content Filter Type

SonicWALL CFS

Note: Enforce the Content Filtering Service per zone from the Network > Zones page.

Restrict Web Features

☐ ActiveX ☐ Java ☐ Cookies ☐ Access to HTTP Proxy Servers ☐ Known Fraudulent Certificates

Trusted Domains

☐ Do not block Java / ActiveX / Cookies to Trusted Domain sites

Name	Configure
No Entries	

Status: Ready

Content Filter Type

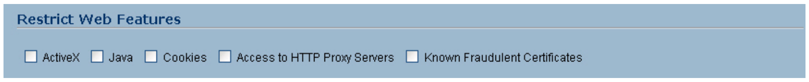
There are three types of content filtering available on the SonicWALL security appliance. These options are available from the **Content Filter Type** menu.

- **SonicWALL CFS** - Selecting **SonicWALL CFS** as the **Content Filter Type** allows you to use the SonicWALL Content Filtering Service that is available as an upgrade. You can obtain more information about SonicWALL Content Filtering Service at <http://www.sonicwall.com/products/cfs.html
- **N2H2** - N2H2 is a third party content filter software package supported by SonicWALL security appliance. You can obtain more information on N2H2 at <http://www.n2h2.com>.
- **Websense Enterprise** - Websense Enterprise is also a third party content filter list supported by SonicWALL security appliance. You can obtain more information on Websense Enterprise at <http://www.websense.com>.

Clicking the **Network>Zones** link in **Note: Enforce the Content Filtering per zone from the Network>Zone page**, displays the **Network>Zones** page for enabling SonicWALL Content Filtering Service on network zones.

Restrict Web Features

Restrict Web Features enhances your network security by blocking potentially harmful Web applications from entering your network.

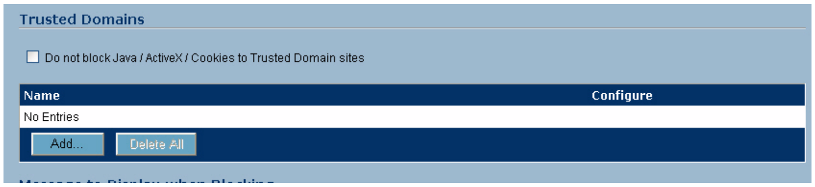

Restrict Web Features
☐ ActiveX
☐ Java
☐ Cookies
☐ Access to HTTP Proxy Servers
☐ Known Fraudulent Certificates

Restrict Web Features are included with SonicOS. Select any of the following applications to block:

- **ActiveX** - ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.
- **Java** - Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.
- **Cookies** - Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.
- **Access to HTTP Proxy Servers** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.
- **Known Fraudulent Certificates** - Digital certificates help verify that Web content and files originated from an authorized party. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates. If digital certificates are proven fraudulent, then the SonicWALL security appliance blocks the Web content and the files that use these fraudulent certificates. Known fraudulent certificates blocked by SonicWALL security appliance include two certificates issued on January 29 and 30, 2001 by VeriSign to an impostor masquerading as a Microsoft employee.

Trusted Domains

Trusted Domains can be added to enable content from specific domains to be exempt from **Restrict Web Features**.


Trusted Domains
☐ Do not block Java / ActiveX / Cookies to Trusted Domain sites
Add...
Delete All

Name	Configure
No Entries	

If you trust content on specific domains and want them exempt from **Restrict Web Features**, follow these steps to add them:

1. Select **Don't block Java/ActiveX/Cookies to Trusted Domains**.
2. Click **Add**. The **Add Trusted Domain Entry** window is displayed.
3. Enter the trusted domain name in the **Domain Name** field.
4. Click **OK**. The trusted domain entry is added to the Trusted Domain table.

To keep the trusted domain entries but enable Restrict Web Features, uncheck **Don't block Java/ ActiveX/Cookies to Trusted Domains**.

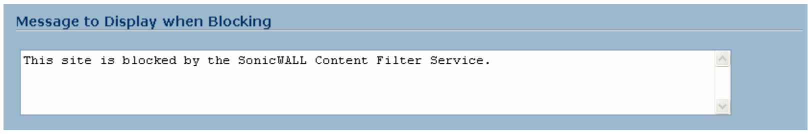
To delete an individual trusted domain, click on the **Trashcan** icon for the entry.

To delete all trusted domains, click **Delete All**.

To edit a trusted domain entry, click the **Notepad** icon.

Message to Display when Blocking

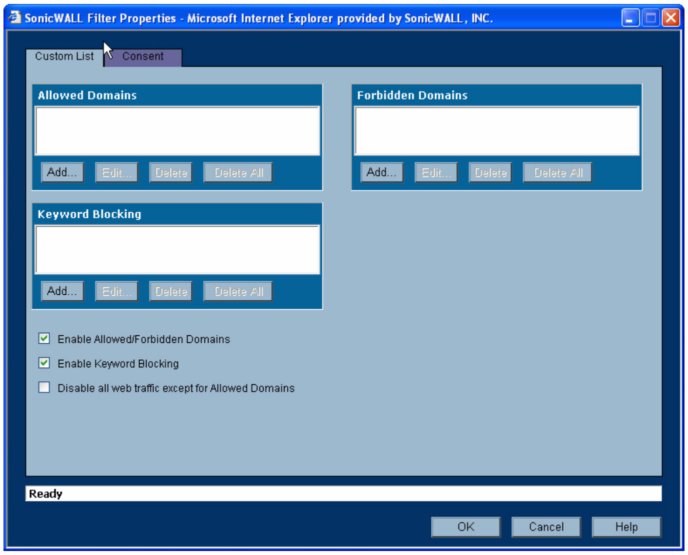
You can enter your customized text to display to the user when access to a blocked site is attempted. The default message is **This site is blocked by the SonicWALL Content Filter Service**. Any message, including embedded HTML, up to 255 characters long, can be entered in this field.


Message to Display when Blocking

This site is blocked by the SonicWALL Content Filter Service.

Configuring SonicWALL Filter Properties

You can customize SonicWALL filter features included with SonicOS from the **SonicWALL Filter Properties** window. To display the **SonicWALL Filter Properties** window, select **SonicWALL CFS** from the **Content Filter Type** menu on the **Security Services>Content Filter** page, and click **Configure**. The **SonicWALL Filter Properties** window is displayed.


SonicWALL Filter Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
Custom List
Consent
Allowed Domains
Add...
Edit...
Delete
Delete All
Forbidden Domains
Add...
Edit...
Delete
Delete All
Keyword Blocking
Add...
Edit...
Delete
Delete All
OK
Cancel
Help

☑ Enable Allowed/Forbidden Domains

☑ Enable Keyword Blocking

☐ Disable all web traffic except for Allowed Domains

Ready

Custom List

You can customize your URL list to include **Allowed Domains** and **Forbidden Domains**. By customizing your URL list, you can include specific domains to be accessed, blocked, and include specific keywords to block sites. Select the check box **Enable Allowed/Forbidden Domains** to activate this feature.

To allow access to a Web site that is blocked by the Content Filter List, click **Add**, and enter the host name, such as “www.ok-site.com”, into the Allowed Domains fields. 256 entries can be added to the **Allowed Domains** list.

To block a Web site that is not blocked by the **Content Filter Service**, click **Add**, and enter the host name, such as “www.bad-site.com” into the **Forbidden Domains** field. 256 entries can be added to the **Forbidden Domains** list.

Alert: *Do not include the prefix "http://" in either the Allowed Domains or Forbidden Domains the fields. All subdomains are affected. For example, entering "yahoo.com" applies to "mail.yahoo.com" and "my.yahoo.com".*

To remove a trusted or forbidden domain, select it from the appropriate list, and click **Delete**. Once the domain has been deleted, the **Status** bar displays **Ready**.

Enable Keyword Blocking

To enable blocking using **Keywords**, select **Enable Keyword Blocking**.Click **Add**, and enter the keyword to block in the **Add Keyword** field, and click **OK**.

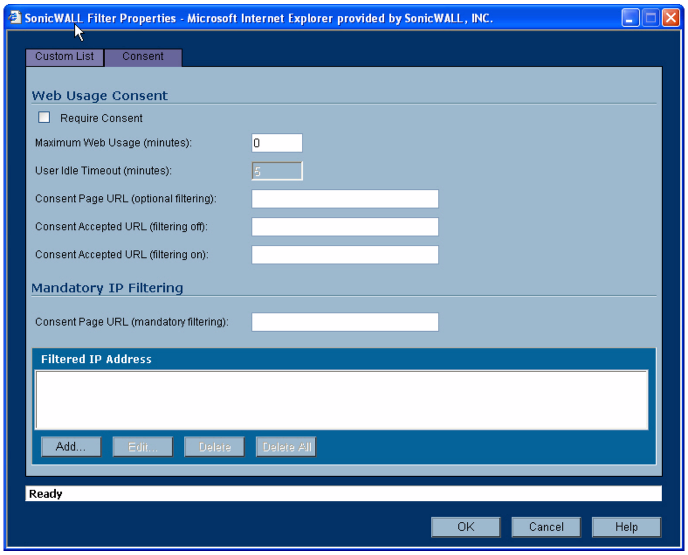
To remove a keyword, select it from the list and click **Delete**. Once the keyword has been removed, the **Status** bar displays **Ready**.

Disable all Web traffic except for Allowed Domains

When the **Disable Web traffic except for Allowed Domains** check box is selected, the SonicWALL security appliance only allows Web access to sites on the **Allowed Domains** list. With careful screening, this can be nearly 100% effective at blocking pornography and other objectionable material.

Consent

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** window before Web browsing is allowed.



☐ Require Consent

Maximum Web Usage (minutes): 0

User Idle Timeout (minutes): 5

Consent Page URL (optional filtering):

Consent Accepted URL (filtering off):

Consent Accepted URL (filtering on):

Consent Page URL (mandatory filtering):

Ready

To enable the **Consent** properties, select **Require Consent**.

- **Maximum Web Usage (minutes) -** In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The SonicWALL security appliance can be used to remind users when their time has expired by displaying the page defined in the **Consent** page URL field. Enter the time limit, in minutes, in the **Maximum Web usage** field. When the default value of zero (0) is entered, this feature is disabled.
- **User Idle Timeout (minutes)** - After a period of Web browser inactivity, the SonicWALL security appliance requires the user to agree to the terms outlined in the Consent page before accessing

the Internet again. To configure the value, follow the link to the Users window and enter the desired value in the User Idle Timeout section.

- **Consent Page URL (optional filtering)** - When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. This page must reside on a Web server and be accessible as a URL by users on the network. It can contain the text from, or links to an Acceptable Use Policy (AUP). This page must contain links to two pages contained in the SonicWALL security appliance, which, when selected, tell the SonicWALL security appliance if the user wishes to have filtered or unfiltered access. The link for unfiltered access must be <192.168.168.168/iAccept.html> and the link for filtered access must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of 192.168.168.168"\.
- **Consent Accepted URL (filtering off)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet without the protection of **Content Filtering**, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering off)** field. This page must reside on a Web server and be accessible as a URL by users on the network.
- **Consent Accepted URL (filtering on)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet with the protection of Content Filtering, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering on)** field. This page must reside on a Web server and be accessible as a URL by users on the network.

Mandatory Filtered IP Addresses

Consent Page URL (mandatory filtering)

When a user opens a Web browser on a computer using mandatory content filtering, a consent page is displayed. You must create the Web page that appears when the Web browser is opened. It can contain text from an Acceptable Use Policy, and notification that violations are logged or blocked.

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWALL security appliance that tells the device that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of 192.168.168.168.

Enter the URL of this page in the **Consent Page URL (mandatory filtering)** field and click **OK**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

Adding a New Address

The SonicWALL security appliance can be configured to enforce content filtering for certain computers on the LAN. Click **Add** to display the **Add Filtered IP Address Entry** window. Enter the IP addresses of these computers in the **Add New Address** field and click **Submit** button. Up to 128 IP addresses can be entered.

To remove a computer from the list of computers to be filtered, highlight the IP address in the **Mandatory Filtered IP Addresses** list and click **Delete.**

CHAPTER 40

Activating SonicWALL Network Anti-Virus

Security Services>Anti-Virus

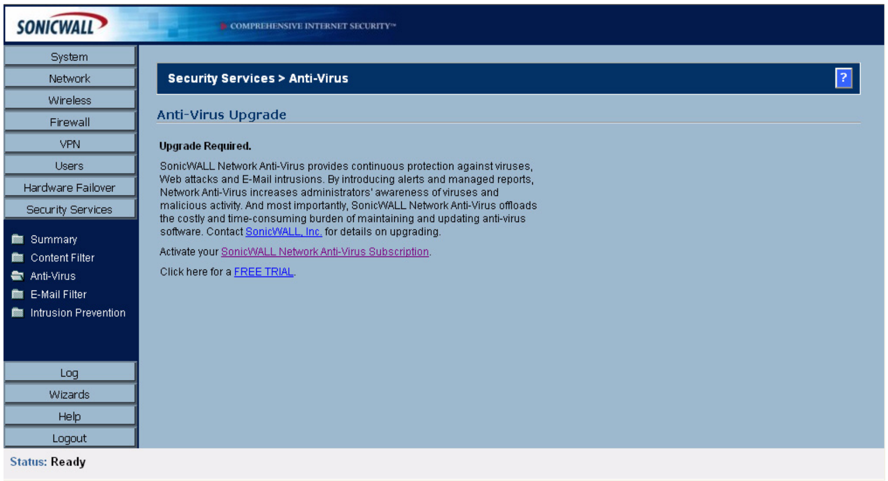
By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses don’t have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

The widespread outbreaks of viruses, such as NIMDA and Code Red, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. SonicWALL Network Anti-Virus prevents occurrences like these and offers a new approach to virus protection. SonicWALL security appliance constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user’s computer. In addition, the SonicWALL security appliance restricts each user’s access to the Internet until they are protected, therefore acting as an enforcer of the company’s virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.

▲ **Alert:** *You must purchase an Anti-Virus subscription to enforce Anti-Virus through the SonicWALL security appliance’s Management Interface.*

Activating SonicWALL Network Anti-Virus

If SonicWALL Network Anti-Virus is not activated, you must activate it.



Security Services > Anti-Virus

Anti-Virus Upgrade

Upgrade Required.

SonicWALL Network Anti-Virus provides continuous protection against viruses, Web attacks and E-Mail intrusions. By introducing alerts and managed reports, Network Anti-Virus increases administrators' awareness of viruses and malicious activity. And most importantly, SonicWALL Network Anti-Virus offloads the costly and time-consuming burden of maintaining and updating anti-virus software. Contact SonicWALL, Inc. for details on upgrading.

Activate your SonicWALL Network Anti-Virus Subscription.

Click here for a FREE TRIAL.

Status: Ready

If you do not have an Activation Key, you must purchase SonicWALL Network Anti-Virus from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada).

Cross Reference: *For complete SonicWALL Network Anti-Virus documentation, see the SonicWALL Network Anti-Virus Administrator's Guide available on your Resource CD or online at http://www.sonicwall.com/services/documentation.html.*

If you have an Activation Key for your SonicWALL Network Anti-Virus subscription, follow these steps to activate SonicWALL Network Anti-Virus:

Alert: *You must have a mySonicWALL.com account and your SonicWALL must be registered to activate SonicWALL Network Anti-Virus.*

1. Click the **SonicWALL Network Anti-Virus Subscription** link on the **Security Services>Anti-Virus** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **SonicWALL Network Anti-Virus Subscription** link.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL Network Anti-Virus subscription is activated on your SonicWALL security appliance.
4. If you activated SonicWALL Network Anti-Virus at www.mySonicWALL.com, the SonicWALL Network Anti-Virus activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services>Summary** page to update your SonicWALL security appliance.

Activating a SonicWALL Network Anti-Virus FREE TRIAL

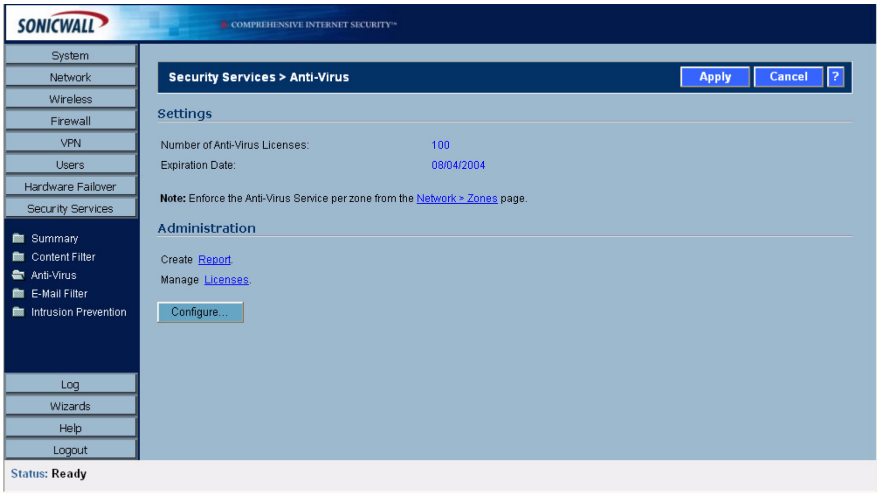
You can try a FREE TRIAL of SonicWALL Network Anti-Virus by following these steps:

1. Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL

security appliance is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **FREE TRIAL** link.

3 Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL Network Anti-Virus subscription is activated on your SonicWALL security appliance.

4 Select **Security Services>Anti-Virus** to display the Anti-Virus page for configuring your SonicWALL Network Anti-Virus settings.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Summary
Content Filter
Anti-Virus
E-Mail Filter
Intrusion Prevention
Log
Wizards
Help
Logout
Security Services > Anti-Virus
Apply
Cancel
?
Configure...

Settings

Number of Anti-Virus Licenses: 100

Expiration Date: 08/04/2004

Note: Enforce the Anti-Virus Service per zone from the Network > Zones page.

Administration

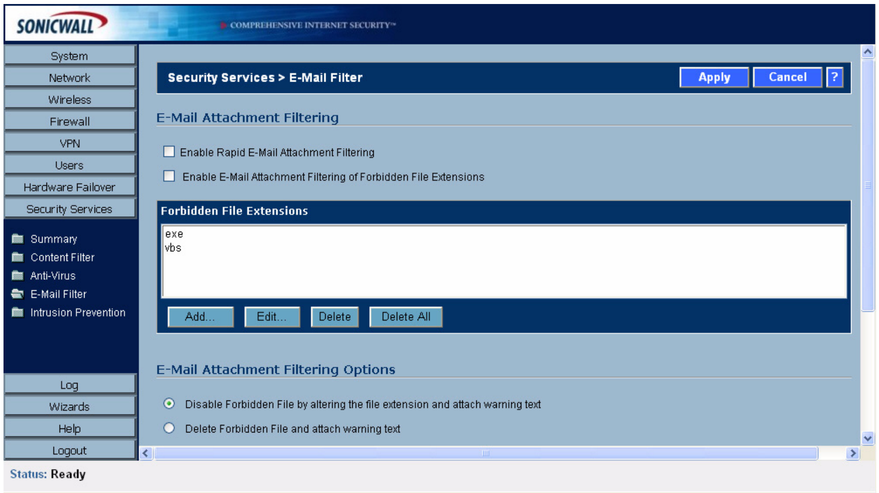
Create Report.

Manage Licenses.

Status: **Ready**

Security Services>E-Mail Filter

The **E-Mail Filter** allows the administrator to selectively delete or disable inbound e-mail attachments as they pass through the SonicWALL security appliance. This feature provides control over executable files and scripts, and applications sent as e-mail attachments.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Summary
Content Filter
Anti-Virus
E-Mail Filter
Intrusion Prevention
Log
Wizards
Help
Logout
Security Services > E-Mail Filter
Apply
Cancel
?
Add...
Edit...
Delete
Delete All

E-Mail Attachment Filtering

☐ Enable Rapid E-Mail Attachment Filtering

☐ Enable E-Mail Attachment Filtering of Forbidden File Extensions

Forbidden File Extensions

exe
vbs

E-Mail Attachment Filtering Options

● Disable Forbidden File by altering the file extension and attach warning text

○ Delete Forbidden File and attach warning text

Status: **Ready**

Note: *E-Mail Filter is included with Network Anti-Virus. When you activate SonicWALL Network Anti-Virus, E-Mail Filter is automatically activated.*

Cross Reference: *For complete SonicWALL Network Anti-Virus documentation including E-Mail Filter, see the SonicWALL Network Anti-Virus Administrator's Guide available on your Resource CD or online at http://www.sonicwall.com/services/documentation.html.*

CHAPTER

41

Activating Intrusion Prevention Service

Security Services > Intrusion Prevention

SonicWALL Intrusion Prevention Service (SonicWALL IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWALL IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWALL's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWALL IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWALL's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

Note: *SonicWALL Intrusion Prevention Service is available for the SonicWALL TZ 170 and PRO Series (PRO 2040, PRO 3060, PRO 4060, and PRO 5060) SonicWALL Internet Security Appliances running SonicOS Standard or Enhanced 2.2 (or higher).*

SonicWALL IPS Features

- **High Performance Deep Packet Inspection Technology** - SonicWALL's Intrusion Prevention Service features a configurable, high-performance Deep Packet Inspection engine that uses parallel searching algorithms on incoming packets through the application layer to deliver increased attack prevention capabilities over those supplied by traditional stateful packet inspection firewall. By performing all of the matching on packets, SonicWALL IPS eliminates the overhead of having to reassemble the data stream. Parallel processing reduces the impact on the processor and maximizes available memory for exceptional performance on SonicWALL appliances.
- **Inter-Zone Intrusion Prevention** - SonicWALL IPS provides an additional layer of protection against malicious threats by allowing administrator's to enforce intrusion prevention not only between each network zone and the Internet, but also between internal network zones. This is performed by enabling intrusion prevention on inbound and outbound traffic between trusted zones (SonicOS Enhanced).
- **Extensive Signature Database** - SonicWALL IPS utilizes an extensive database of over 1,700 attack and vulnerability signatures written to detect and prevent intrusions, worms, application exploits, as well as peer-to-peer and instant messaging traffic. The SonicWALL Deep Packet

Inspection engine can also read signatures written in the popular Snort format, allowing SonicWALL to easily incorporate new signatures as they are published by third parties. SonicWALL maintains a current and robust signature database by incorporating the latest available signatures from thousands of open source developers and by continually developing new signatures for application vulnerabilities that are not immediately available or provided by open source.

- **Dynamically Updated Signature Database** - SonicWALL IPS includes automatic signature updates delivered through SonicWALL's Distributed Enforcement Architecture (DEA), providing protection from emerging threats and lowering total cost of ownership. Updates to the signature database are dynamic for SonicWALL firewalls under an active subscription.
- **Scalable** - SonicWALL IPS is a scalable solution for SonicWALL TZ 170 and PRO Series Appliances that secures small, medium and large networks with complete protection from application exploits, worms and malicious traffic.
- **Application Control** - SonicWALL IPS provides the ability to prevent Instant Messaging and Peer-to-Peer file sharing programs from operating through the firewall, closing a potential backdoor that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.
- **Simplified Deployment and Management** - SonicWALL IPS allows network administrators to quickly and easily manage the service within minutes. Administrator's can create global policies between security zones and interfaces as well as group attacks by priority, simplifying deployment and management across a distributed network.
- **Granular Policy Management** - SonicWALL IPS provides administrators with a range of granular policy tools to enforce IPS on a global, group, or individual signature level to enable more control and reduce the number of false policies. SonicWALL IPS allows also allows administrators to choose between detection, prevention, or both to tailor policies for their specific network environment.
- **Logging and Reporting** - SonicWALL IPS offers comprehensive logging of all intrusion attempts with the ability to filter logs based on priority level, enabling administrator's to highlight high priority attacks. Granular reporting based on attack source, destination and type of intrusion is available through SonicWALL ViewPoint and Global Management System. A hyperlink of the intrusion brings up the signature window for further information from the SonicWALL appliance log.
- **Management by Risk Category** - SonicWALL IPS allows you to enable/disable detection or prevention based on the priority level of attack through High, Medium, or Low predefined priority groups.
- **Detection Accuracy** - SonicWALL IPS detection and prevention accuracy is achieved minimizing both false positives and false negatives. Signatures are written around applications, such as Internet Explorer or SQL Server rather than ports or protocols to ensure that malicious code targeting them are correctly identified and prevented.

SonicWALL Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

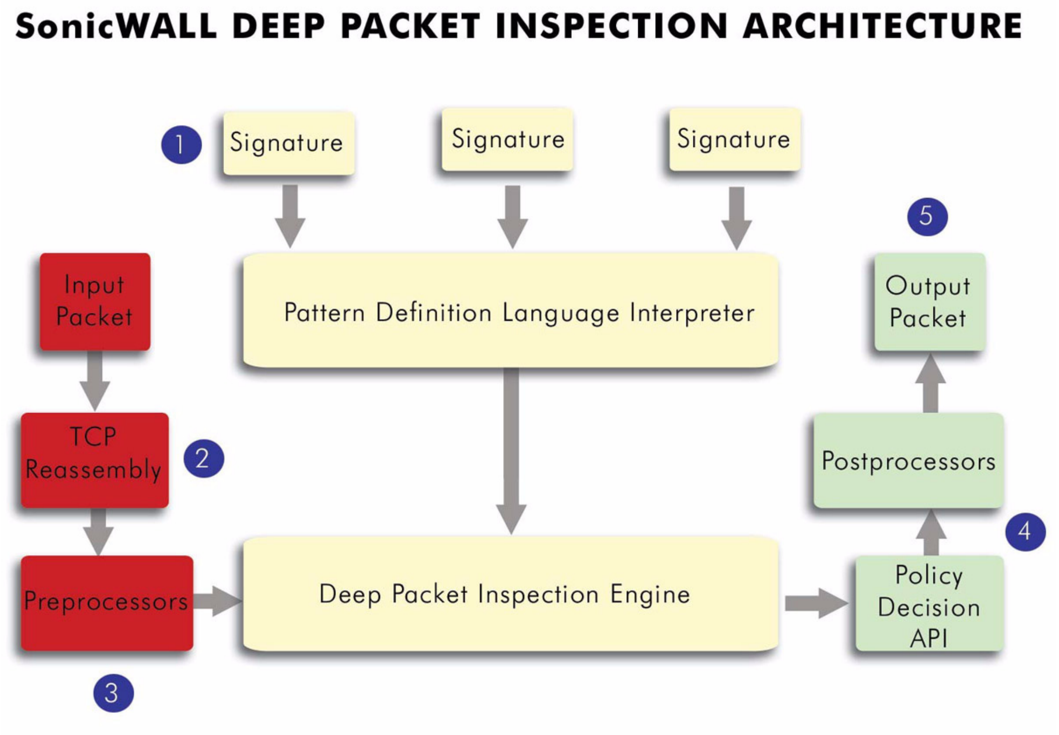
Deep Packet Inspection is a technology that allows a SonicWALL Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWALL Security Appliance, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWALL's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

How SonicWALL's Deep Packet Inspection Works

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWALL Intrusion Prevention Service. SonicWALL's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture.

The following steps describe how the SonicWALL Deep Packet Inspection Architecture works:

1. Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
2. TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
3. Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.
4. Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or could even reset a TCP connection.
5. SonicWALL's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.


SonicWALL DEEP PACKET INSPECTION ARCHITECTURE
1
Signature
Signature
Signature
5
Input Packet
Pattern Definition Language Interpreter
Output Packet
TCP Reassembly
2
Postprocessors
4
Preprocessors
Deep Packet Inspection Engine
Policy Decision API
3

SonicWALL IPS Terminology

- **Stateful Packet Inspection** - looking at the header of the packet to control access based on port, protocol, and IP address.
- **Deep Packet Inspection** - looking at the data portion of the packet. Enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities.

- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Snort** - an open source network intrusion detection system. SonicWALL IPS includes open-source Snort signatures, as well as signatures from other signature databases, and SonicWALL created signatures. SonicWALL does not use the Snort engine.
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.

SonicWALL IPS Activation

If you do not have SonicWALL IPS activated on your SonicWALL, you must purchase SonicWALL IPS from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you do not have SonicWALL IPS installed on your SonicWALL, the **Security Services>Intrusion Prevention** page indicates an upgrade is required and includes a link to activate your IPS subscription from the SonicWALL Management Interface or to activate a FREE TRIAL of SonicWALL IPS.

Note: *You must have SonicOS Standard or Enhanced 2.2 (or higher) to activate SonicWALL IPS, and your SonicWALL must be registered on https://www.mySonicwall.com.*

mySonicWALL.com

mySonicWALL.com delivers a convenient, one-stop resource for registration, activation, and management of your SonicWALL products and services. Your mySonicWALL.com account provides a single profile to do the following:

- Register your SonicWALL Internet Security Appliances
- Purchase/Activate SonicWALL Security Services and Upgrades
- Receive SonicWALL firmware and security service updates and alerts
- Manage (change or delete) your SonicWALL security services
- Access SonicWALL Technical Support

Creating a mySonicWALL.com account is easy and free. Simply complete an online registration form. Once your account is created, you can register SonicWALL Internet Security Appliances and activate any SonicWALL Security Services associated with the SonicWALL.

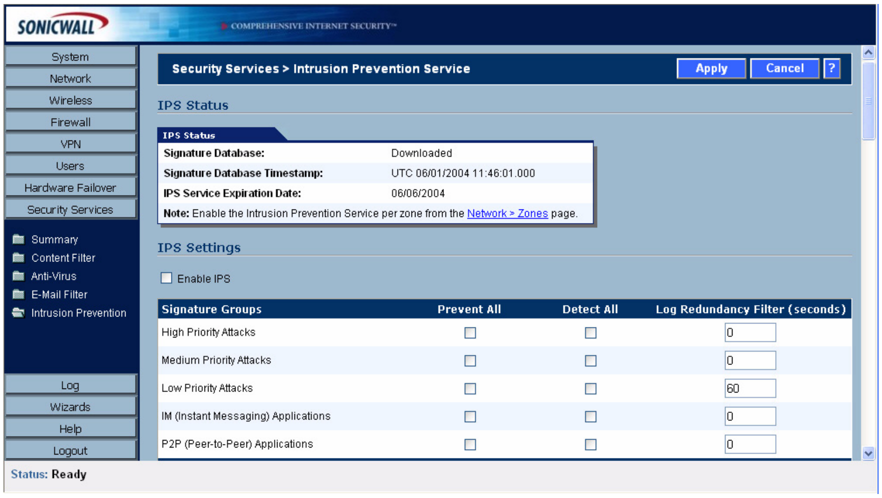
Your mySonicWALL.com account is accessible from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information. You can also access mySonicWALL.com license and registration services directly from the SonicWALL management interface for increased ease of use and simplified services activation.

If you activated SonicWALL IPS at mySonicWALL.com, the SonicWALL IPS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services>Summary** page to update your SonicWALL.

Activating SonicWALL IPS

If you have an Activation Key for your SonicWALL IPS, follow these steps to activate IPS:

1. Click the **SonicWALL IDP Subscription** link on the **Security Services>Intrusion Prevention** page. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL is already registered to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **SonicWALL IPS Subscription** link.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL IPS subscription is activated on your SonicWALL.
4. Select **Security Services>Intrusion Prevention** to display the **Intrusion Prevention Service** page for configuring your IPS settings.



Security Services > Intrusion Prevention Service

IPS Status

IPS Status

Signature Database:	Downloaded
Signature Database Timestamp:	UTC 06/01/2004 11:46:01.000
IPS Service Expiration Date:	06/06/2004

Note: Enable the Intrusion Prevention Service per zone from the Network > Zones page.

IPS Settings

☐ Enable IPS

Signature Groups	Prevent All	Detect All	Log Redundancy Filter (seconds)
High Priority Attacks	☐	☐	0
Medium Priority Attacks	☐	☐	0
Low Priority Attacks	☐	☐	60
IM (Instant Messaging) Applications	☐	☐	0
P2P (Peer-to-Peer) Applications	☐	☐	0

Status: Ready

If you activated the SonicWALL IPS subscription on mySonicWALL.com, the SonicWALL IPS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services>Summary** page to update your SonicWALL.

Activating the SonicWALL IPS FREE TRIAL

To try a FREE TRIAL of SonicWALL IPS, follow these steps:

1. Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **FREE TRIAL** link.
3. Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL IPS trial subscription is activated on your SonicWALL.

PART

10

Log

:

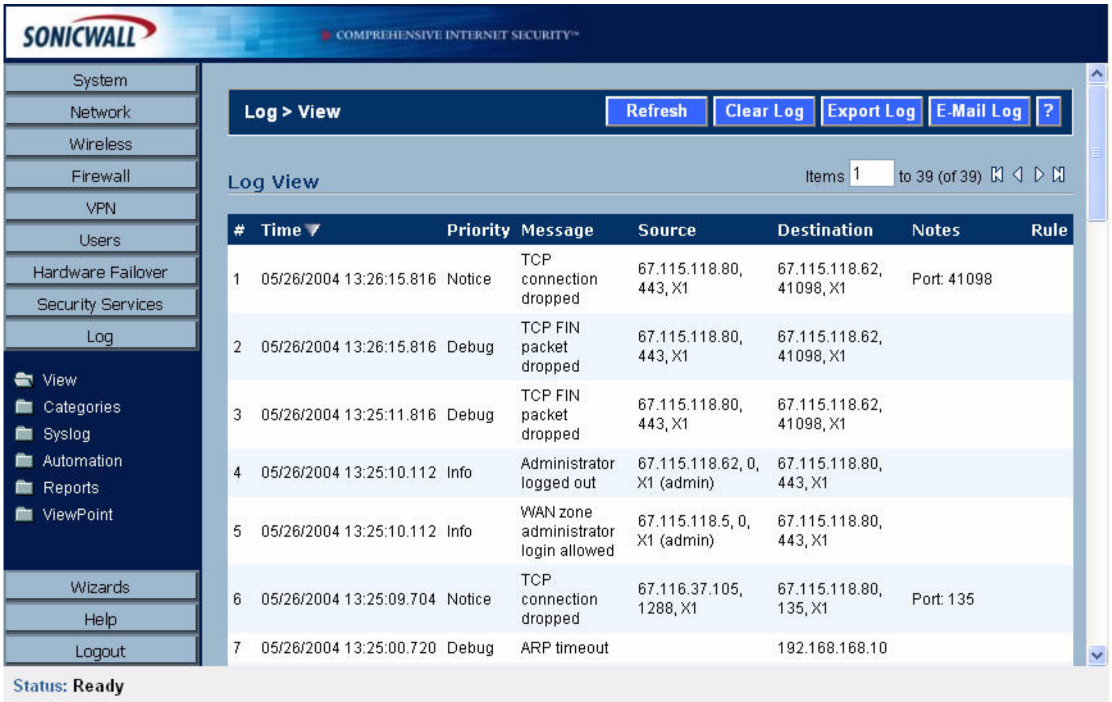
CHAPTER 42

Managing Log Events

Log > View

The SonicWALL security appliance maintains an Event log for tracking potential security threats. This log can be viewed in the **Log > View** page, or it can be automatically sent to an e-mail address for convenience and archiving. The log is displayed in a table and can be sorted by column.

The SonicWALL security appliance can alert you of important events, such as an attack to the SonicWALL security appliance. Alerts are immediately e-mailed, either to an e-mail address or to an e-mail pager. Each log entry contains the date and time of the event and a brief message describing the event.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
View
Categories
Syslog
Automation
Reports
ViewPoint
Wizards
Help
Logout
Log > View
Refresh
Clear Log
Export Log
E-Mail Log
?
Log View
Items 1 to 39 (of 39)
Status: Ready

#	Time	Priority	Message	Source	Destination	Notes	Rule
1	05/26/2004 13:26:15.816	Notice	TCP connection dropped	67.115.118.80, 443, X1	67.115.118.62, 41098, X1	Port: 41098	
2	05/26/2004 13:26:15.816	Debug	TCP FIN packet dropped	67.115.118.80, 443, X1	67.115.118.62, 41098, X1		
3	05/26/2004 13:25:11.816	Debug	TCP FIN packet dropped	67.115.118.80, 443, X1	67.115.118.62, 41098, X1		
4	05/26/2004 13:25:10.112	Info	Administrator logged out	67.115.118.62, 0, X1 (admin)	67.115.118.80, 443, X1		
5	05/26/2004 13:25:10.112	Info	WAN zone administrator login allowed	67.115.118.5, 0, X1 (admin)	67.115.118.80, 443, X1		
6	05/26/2004 13:25:09.704	Notice	TCP connection dropped	67.116.37.105, 1288, X1	67.115.118.80, 135, X1	Port: 135	
7	05/26/2004 13:25:00.720	Debug	ARP timeout		192.168.168.10		

Log View Table

The log is displayed in a table and is sortable by column. The log table columns include:

- **Time** - the date and time of the event.
- **Priority** - the level of priority associated with your log event.
  Syslog uses eight categories to characterize messages – in descending order of severity, the categories include:
  - Emergency
  - Alert
  - Critical
  - Error
  - Warning
  - Notice
  - Informational
  - Debug

  Specify a priority level on a SonicWALL security appliance on the **Log** > **Categories** page to log messages for that priority level, plus all messages tagged with a higher severity. For example, select ‘error’ as the priority level to log all messages tagged as ‘error,’ as well as any messages tagged with ‘critical,’ ‘alert,’ and ‘emergency.’ Select ‘debug’ to log all messages.

Cross Reference: *Refer to Log Event Messages section for more information on your specific log event.*

- **Message** - provides description of the event.
- **Source** - displays source network and IP address.
- **Destination** - displays the destination network and IP address.
- **Notes** - provides additional information about the event.
- **Rule** - notes Network Access Rule affected by event.

Navigating and Sorting Log View Table Entries

The **Log View** table provides easy pagination for viewing large numbers of log events. You can navigate these log events by using the navigation control bar located at the top right of the **Log View** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Refresh

To update log messages, clicking the **Refresh** button.

Clear Log

To delete the contents of the log, click the **Clear Log** button.

Export Log

To export the contents of the log to a defined destination, click the **Export Log** button.You can export log content to two formats:

- **Plain text format**--Used in log and alert email.
- **Comma-separated value** (**CSV**) **format**--Used for importing into Excel or other presentation development applications.

E-mail Log

If you have configured the SonicWALL security appliance to e-mail log files, clicking **E-mail Log** sends the current log files to the e-mail address specified in the **Log > Automation > E-mail** section.

Note: *The SonicWALL security appliance can alert you of important events, such as an attack to the SonicWALL security appliance. Alerts are immediately sent via e-mail, either to an e-mail address or to an e-mail pager. For sending alerts, you must enter your e-mail address and server information in the Log>Automation page.*

Log Event Messages

This section provides log event descriptions listed by Priority and by chronological order of the Message ID.

Refer to the following tables for log messages by priority level:

- Alert Log Messages
- Critical Log Messages
- Error Log Messages
- Warning Log Messages
- Notice Event Logs
- Info Log Messages
- Debug Log Messages

Emergency logs, the highest priority logs, are not listed.

Alert Log Messages

Message ID	Priority	Description of Log Event
29	Alert	Administrator login allowed
30	Alert	Administrator login denied
31	Alert	Local user login allowed
32	Alert	Local user login denied
33	Alert	User login denied
34	Alert	Login screen timed out
35	Alert	Administrator login denied from %s
199	Alert	CLI administrator login allowed
200	Alert	CLI administrator login denied
235	Alert	VPN zone administrator login allowed
236	Alert	WAN zone administrator login allowed
237	Alert	VPN zone remote user login allowed

Critical Log Messages

Message ID	Log Event	Priority	Description of Log Event
238	logstrSuccessfulUserWanLogin	Critical	WAN zone remote user login allowed
261	logstrAdminLogout	Critical	Administrator logged out

Error Log Messages

Message ID	Log Event	Priority	Description of Log Event
4	logstrActivated	Error	SonicWALL activated
5	logstrLogLogCleared	Error	Log Cleared
6	logstrLogSentToEmail	Error	Log successfully sent via email
7	logstrLogFull	Error	Log full; deactivating SonicWALL
12	logstrLogProblemEmailingCheckSettings	Error	Problem sending log email; check log settings
13	logstrRestartingDumpingLog	Error	Restarting SonicWALL; dumping log to email
53	logstrCacheFull	Error	The cache is full; %u open connections; some will be dropped
58	logstrConnDroppedTooManyIP	Error	License exceeded: Connection dropped because too many IP addresses are in use on your LAN
64	logstrInternalErr	Error	Diagnostic Code D
93	logstrLogSuspendReboot	Error	Diagnostic Code A
94	logstrLogDeadlockReboot	Error	Diagnostic Code B
95	logstrLogLowMemReboot	Error	Diagnostic Code C
114	logstrDHCPCBoundRenew	Error	DHCP Client sending REQUEST and going to RENEW state.
115	logstrDHCPCRequestRenew	Error	Sending DHCP REQUEST (Renewing).
116	logstrDHCPCRequestRebind	Error	Sending DHCP REQUEST (Rebinding).
117	logstrDHCPCRequestReboot	Error	Sending DHCP REQUEST (Rebooting).
118	logstrDHCPCRequestVerify	Error	Sending DHCP REQUEST (Verifying).

Message ID	Log Event	Priority	Description of Log Event
119	logstrDHCPCVerifyFailInit	Error	DHCP Client failed to verify and lease has expired. Go to INIT state.
120	logstrDHCPCVerifyFailBound	Error	DHCP Client failed to verify and lease is still valid. Go to BOUND state.
121	logstrDHCPCGotNewIP	Error	DHCP Client got a new IP address lease.
122	logstrDHCPCSendRelease	Error	Sending DHCP RELEASE.
142	logstrLogDebug	Error	Log Debug
143	logstrLogAddTest	Error	Add an attack message
164	logstrLogHttpServerReboot	Error	Diagnostic Code F
198	logstrFirmwareUpdateEmailSubject	Error	New firmware available.
222	logstrDhcprRemoteRelease	Error	DHCP RELEASE relayed to Central Gateway
223	logstrDhcprRemoteAck	Error	DHCP lease relayed to local device
224	logstrDhcprCentralRelease	Error	DHCP RELEASE received from remote device
225	logstrDhcprCentralAck	Error	DHCP lease relayed to remote device
226	logstrDhcprAckConflict	Error	DHCP lease to LAN device conflicts with remote device, deleting remote IP entry
227	logstrDhcprAckInStaticTable	Error	WARNING: DHCP lease relayed from Central Gateway conflicts with IP in Static Devices list
228	logstrDhcprAckIsRelay	Error	DHCP lease dropped. Lease from Central Gateway conflicts with Relay IP
229	logstrDhcprIpSpoof	Error	IP spoof detected on packet to Central Gateway, packet dropped
230	logstrDhcprRemoteGetTable	Error	Request for Relay IP Table from Central Gateway
231	logstrDhcprCentralGetTable	Error	Requesting Relay IP Table from Remote Gateway
232	logstrDhcprRemoteSentTable	Error	Sent Relay IP Table to Central Gateway
233	logstrDhcprCentralRcvTable	Error	Obtained Relay IP Table from Remote Gateway
234	logstrDhcprTableReqTimedOut	Error	Failed to synchronize Relay IP Table
325	logstrWanLinkDown	Error	The current WAN interface is not ready to route packets.
332	logstrEtherPortUp	Error	%s Ethernet Port Up
333	logstrEtherPortDown	Error	%s Ethernet Port Down
340	logstrHttpPortChange	Error	HTTP management port has changed
341	logstrHttpsPortChange	Error	HTTPS management port has changed
348	logstrImportedSAInvalid	Error	Imported VPN SA is invalid - disabled
374	logstrVpnHwInitErr	Error	Error initializing Hardware acceleration for VPN

Message ID	Log Event	Priority	Description of Log Event
472	logstrDhcprNoRelayIpAvailable	Error	WARNING: Central Gateway does not have a Relay IP Address. DHCP message dropped.
473	logstrDhcprRequestMessage	Error	DHCP REQUEST received from remote device
474	logstrDhcprDiscoverMessage	Error	DHCP DISCOVER received from remote device
475	logstrDhcprDeclineMessage	Error	DHCP DECLINE received from remote device
476	logstrDhcprOfferMessage	Error	DHCP OFFER received from server
477	logstrDhcprServerNakMessage	Error	DHCP NAK received from server
478	logstrDhcpOverVpnTunnelNotDefined	Error	ERROR: DHCP over VPN policy is not defined. Cannot start IKE.
479	logstrDhcprDiscoverLocal	Error	DHCP DISCOVER received from local device
480	logstrDhcprRequestLocal	Error	DHCP REQUEST received from local device
484	logstrDhcprAckIsRemoteMgmt	Error	DHCP lease dropped. Lease from Central Gateway conflicts with Remote Management IP
493	logStrISDNUpdated	Error	ISDN Driver Firmware successfully updated
498	logstrWanNotSetup	Error	WAN Interface not setup
502	logstrWANNotReady	Error	WAN not ready
504	logstrDHCPNotReady	Error	DHCP client enabled but not ready
517	logstrLogWlanReboot	Error	Diagnostic Code D
521	logstrInitializing	Error	SonicWALL initializing
530	logstrNATDisabled	Error	Network Modem Mode Enabled: turning off NAT
531	logstrNATEnabled	Error	Network Modem Mode Disabled: re-enabling NAT
539	logStrRtcBatteryDead1	Error	Real time clock battery failure. Time values may be incorrect
540	logStrRtcBatteryDead2	Error	If not already enabled, enabling NTP is recommended
541	logStrBwmLimitOnUpgrade	Error	Maximum number of Bandwidth Managed rules exceeded upon upgrade to this version. Some Bandwidth settings ignored.
565	logstrMultiIfLinkUp	Error	Interface %s Link Is Up
566	logstrMultiIfLinkDown	Error	Interface %s Link Is Down
567	logstrIfProtoShutdown	Error	Interface IP Assignment changed: Shutting down %s
568	logstrIfProtoBindInit	Error	Interface IP Assignment: Binding and initializing %s
569	logstrNetworkOverlap	Error	Network for interface %s overlaps with another interface.
570	logStrInvalidNetwork	Error	Please connect interface %s to another network to function properly

Message ID	Log Event	Priority	Description of Log Event
572	logStrOlderPrefs	Error	A prior version of preferences was loaded because the most recent preferences file was inaccessible
573	logStrPrefsTooBig	Error	The preferences file is too large to be saved in available flash memory
574	logStrPrefsDefaulted	Error	All preference values have been set to factory default values
575	logstrSysEnvVoltageFail	Error	Voltages Out of Tolerance
576	logstrSysEnvFanFail	Error	Fan Failure
577	logstrSysEnvTempYellow	Error	Thermal Yellow
578	logstrSysEnvTempRed	Error	Thermal Red
579	logstrSysEnvTempRedExceed	Error	Thermal Red Timer Exceeded
588	logstrDHCPCOfferError	Error	Received DHCP offer packet has errors
589	logstrDHCPCRequestResponseError	Error	Received response packet for DHCP request has errors
599	logstrLogStackMarginReboot	Error	Diagnostic Code G
600	logstrLogDeleteReboot	Error	Diagnostic Code H
601	logstrLogDeleteStackReboot	Error	Diagnostic Code I
611	logstrStdToEnhUpgrade1	Error	A SonicOS Standard to Enhanced Upgrade was performed
612	logstrStdToEnhUpgrade2	Error	Not all configurations may have been completely upgraded
613	logstrStdToEnhUpgrade3	Error	Please manually check all system configurations for correctness of Upgrade
654	logstrLogEventRateExceeded	Error	Maximum events per second threshold exceeded

Warning Log Messages

Message ID	Log Event	Priority	Description of Log Event
61	logstrLogOutOfMemory	Warning	Diagnostic Code E
62	logstrLogIpsecDynamicHostConnect	Warning	Dynamic IPSec client connected
65	logstrLogIllegalSpi	Warning	Illegal IPSec SPI
66	logstrLogUnknownSpi	Warning	Unknown IPSec SPI
67	logstrLogIpsecAuthFailure	Warning	IPSec Authentication Failed
68	logstrLogIpsecDecryptFailure	Warning	IPSec Decryption Failed
69	logstrLogIncompatibleSA	Warning	Incompatible IPSec Security Association
70	logstrLogIllegalIpsecPeer	Warning	IPSec packet from or to an illegal host
180	logstrReplayDetected	Warning	IPSEC Replay Detected

Message ID	Log Event	Priority	Description of Log Event
239	logstrVpnNatTravPeerBehindNat	Warning	NAT Discovery: Peer IPSec Security Gateway behind a NAT/ NAPT Device
240	logstrVpnNatTravWeBehindNat	Warning	NAT Discovery: Local IPSec Security Gateway behind a NAT/ NAPT Device
241	logstrVpnNatTravNoNatDevicePresent	Warning	NAT Discovery: No NAT/NAPT device detected between IPSec Security gateways
242	logstrVpnNatTravPeerNotSupportNatTraversal	Warning	NAT Discovery: Peer IPSec Security Gateway doesn't support VPN NAT Traversal
247	logstrLogIllegalPktFromIpsecPeer	Warning	IPSec packet from an illegal host
256	logstrLogIkeProposalLanAddrOnDmz	Warning	IKE Responder: Tunnel terminates on DMZ but proposed local network is on LAN
257	logstrLogIkeProposalDmzAddrOnLan	Warning	IKE Responder: Tunnel terminates on LAN but proposed local network is on DMZ
258	logstrLogIkeProposalAhPfsMismatch	Warning	IKE Responder: AH Perfect Forward Secrecy mismatch
259	logstrLogIkeProposalEspPfsMismatch	Warning	IKE Responder: ESP Perfect Forward Secrecy mismatch
260	logstrLogIkeProposalAlgKeyMismatch	Warning	IKE Responder: Algorithms and/or keys do not match
266	logstrIpsecAHNatMaynotWork	Warning	NAT device may not support IPSec AH pass through
269	logstrCrlRequest	Warning	Requesting CRL from
270	logstrCrlDownloadSuccess	Warning	CRL Loaded from
271	logstrCrlDownloadFailed	Warning	Failed to get CRL from
272	logstrCrlFailNoMem	Warning	Not enough memory to hold the CRL
273	logstrCrlFailTimedOut	Warning	Connection timed out
274	logstrCrlFailNoConnect	Warning	Cant connect to the CRL server
275	logstrCrlFailNoReason	Warning	Unknown reason
276	logstrCrlProcFail	Warning	Failed to Process CRL from
277	logstrCrlBadFormat	Warning	Bad CRL format
278	logstrCrlWrongIssuer	Warning	Issuer match failed
279	logstrCrlCertRevoked	Warning	Certificate on Revoked list (CRL)
280	logstrNoCertificate	Warning	No Certificate for

Message ID	Log Event	Priority	Description of Log Event
307	logstrWanModeIs	Warning	The network connection in use is %s
326	logstrWfoProbeFailed	Warning	Probing failure on %s
342	logstrLogIkeProposalBadModeForXauth	Warning	IKE Responder: Mode %d - not transport mode. Xauth is required but not supported by peer.
345	logstrLogIkeProposalOutsideRemNotNat	Warning	IKE Responder: Tunnel terminates outside firewall but proposed remote network is not NAT public address
346	logstrLogIkeBeginInitiatorPh2	Warning	IKE Initiator: Start Quick Mode (Phase 2).
349	logstrIpsecSaLifetimeExpired	Warning	IPSEC SA lifetime expired.
350	logstrIkeSaLifetimeExpired	Warning	IKE SA lifetime expired.
351	logstrStartMMIkeNegotiation	Warning	IKE Initiator: Start Main Mode negotiation (Phase 1)
352	logstrReceiveQMRequest	Warning	IKE Responder: Received Quick Mode Request (Phase 2)
353	logstrInitMMPhase1Complete	Warning	IKE Initiator: Main Mode complete (Phase 1)
354	logstrInitAMPhase1Complete	Warning	IKE Initiator: Aggressive Mode complete (Phase 1).
355	logstrRespMMIkeRequest	Warning	IKE Responder: Received Main Mode request (Phase 1)
356	logstrRespAMIkeRequest	Warning	IKE Responder: Received Aggressive Mode request (Phase 1)
357	logstrRespMMPhase1Complete	Warning	IKE Responder: Main Mode complete (Phase 1)
358	logstrStartAMIkeNegotiation	Warning	IKE Initiator: Start Aggressive Mode negotiation (Phase 1)
434	logstrWfoManualSecProfile	Warning	PPP Dial-Up: Trying to failover but Alternate Profile is manual
435	logstrWfoFailback	Warning	WLB Failback initiated by %s
436	logstrWfoProbeSuccess	Warning	Probing succeeded on %s
445	logstrAcceptingResponderLifetime	Warning	IKE Initiator: Accepting peer lifetime. (Phase 1)
447	logPkeFailure	Warning	PKI Failure
448	logPkeOutputLen	Warning	PKI Failure: Output buffer too small
449	logPkeAlloc	Warning	PKI Failure: Cannot alloc memory

Message ID	Log Event	Priority	Description of Log Event
450	logPkeEntityCertLimit	Warning	PKI Failure: Reached the limit for local certs, cannot load any more
451	logPkeImportFailed	Warning	PKI Failure: Import failed
452	logPkeBadPassword	Warning	PKI Failure: Incorrect admin password
453	logPkeCaCertLimit	Warning	PKI Failure: CA certificates store exceeded. Cannot verify this Local Certificate
454	logPkeBadPkcs12Import	Warning	PKI Failure: Improper file format. Please select PKCS#12 (*.p12) file
455	logPkeNonSonicId	Warning	PKI Failure: Certificate's ID does not match this SonicWall
456	logPkePubPrivKeyMismatch	Warning	PKI Failure: public-private key mismatch
457	logPkeDupLocalCertName	Warning	PKI Failure: Duplicate local certificate name
458	logPkeDupLocalCert	Warning	PKI Failure: Duplicate local certificate
459	logPkeNoCa	Warning	PKI Failure: No CA certificates yet loaded
460	logPkeDataStoreCorrupt	Warning	PKI Failure: Internal error
461	logPkeNoResource	Warning	PKI Failure: Temporary memory shortage, try again
462	logPkeChainCircular	Warning	PKI Failure: The certificate chain is circular
463	logPkeChainIncomplete	Warning	PKI Failure: The certificate chain is incomplete
464	logPkeChainNoRoot	Warning	PKI Failure: The certificate chain has no root
465	logPkeAfterTime	Warning	PKI Failure: The certificate or a certificate in the chain has expired
466	logPkeBeforeTime	Warning	PKI Failure: The certificate or a certificate in the chain has a validity period in the future
467	logPkeBadDerCert	Warning	PKI Failure: The certificate or a certificate in the chain is corrupt
468	logPkeBadSig	Warning	PKI Failure: The certificate or a certificate in the chain has a bad signature
469	logPkeCouldNotValidateCert	Warning	PKI Failure: Loaded but could not verify certificate

Message ID	Log Event	Priority	Description of Log Event
470	logPkeCouldNotValidateChain	Warning	PKI Failure: Loaded the certificate but could not verify it's chain
483	logstrInvalidId	Warning	Received notify: INVALID_ID_INFO
487	logstrWlanFirmwareUpdated	Warning	wlan firmware image has been updated
488	logstrPktDropByWGuest	Warning	Packet dropped by wlan guest check
495	logstrPktDropByVpnTraversal	Warning	Packet dropped by wlan vpn traversal check
516	logstrLogIkeProposalAddrWithOutDefGw	Warning	IKE Responder: Default LAN gateway is not set but peer is proposing to use this SA as a default route
518	logstrWlan80211bMgmt	Warning	802.11b Management
519	logstrWlanRecover	Warning	wlan recovery
532	logstrPktDropWanRestricted	Warning	Internet Access restricted to authorized users. Dropped packet received in the clear.
533	logstrIpsecEspDropped	Warning	IPSec (ESP) packet dropped
534	logstrIpsecAhDropped	Warning	IPSec (AH) packet dropped
535	logstrSimultIpsecEspConnDropped	Warning	IPSec (ESP) packet dropped; waiting for pending IPSec connection
536	logstrSimultIpsecAhConnDropped	Warning	IPSec (AH) packet dropped; waiting for pending IPSec connection
542	logstrDialupDuration	Warning	PPP Dial-Up: Previous session was connected for %s
543	logstrStartIkeNegSecGateway	Warning	IKE Initiator: Using secondary gateway to negotiate
544	logstrIkeInitIncorrectLocalAddr	Warning	IKE Initiator drop: Packet dest address does not match selected local interface address
545	logstrIkeRespIncorrectLocalAddr	Warning	IKE Responder drop: Packet dest address does not match selected local interface address
546	logstrWlanRogueAP	Warning	Found Rogue Access Point
547	logstrWlanSeqCheck	Warning	wlan sequence number out of order
548	logstrWlanAssoFlood	Warning	Association Flood from wlan station

Message ID	Log Event	Priority	Description of Log Event
556	logstrWlanPassiveRogueAP	Warning	Found Rogue Access Point
581	logstrWlbOnSpill	Warning	WLB Spill-over started, configured threshold exceeded
582	logstrWlbOffSpill	Warning	WLB Spill-over stopped
584	logstrWlbFailover	Warning	WLB Failover in progress
585	logstrWlbResourceAvailable	Warning	WLB Resource is now available
586	logstrWlbResourceFailed	Warning	WLB Resource failed
587	logstrHdrVerifyFailed	Warning	Header verification failed
605	logstrUnencryptedWhileCryptoActive	Warning	Received unencrypted packet while crypto active
607	logstrReceivedOnWrongPort	Warning	Received ISAKMP packet destined to port %s
615	logstrWlanProbeCheck	Warning	WLAN client null probing
616	logstrIKEDetailErrLog	Warning	%s-payload processing error
617	logStrWlanModeDHCPS	Warning	WLAN not in AP mode, DHCP server will not provide lease to clients on WLAN

Notice Log Messages

Message ID	Log Event	Priority	Description of Log Event
87	logstrLogIkeProposalOK	Notice	IKE Responder: Accepting IPSec proposal (Phase 2)
88	logstrLogIpsecProposalReject	Notice	IKE Responder: IPSec proposal does not match (Phase 2)
89	logstrLogIkeAddIPSecSA	Notice	IKE negotiation complete. Adding IPSec SA. (Phase 2)
90	logstrLogIkeStartNegotiation	Notice	Starting IKE negotiation
91	logstrLogIkeDeleteSADstAddr	Notice	Deleting IPSec SA for destination
92	logstrLogIkeDeleteSASpi	Notice	Deleting IPSec SA
249	logstrLogIkeProposalBadMode	Notice	IKE Responder: Mode %d - not tunnel mode
250	logstrLogIkeProposalPhase1IdMismatch	Notice	IKE Responder: No matching Phase 1 ID found for proposed remote network
251	logstrLogIkeProposalBadZeroRemAddr	Notice	IKE Responder: Proposed remote network is 0.0.0.0 but not DHCP relay nor default route
252	logstrLogIkeProposalNoRemNetMatch	Notice	IKE Responder: No match for proposed remote network address

Message ID	Log Event	Priority	Description of Log Event
253	logstrLogIkeProposalAddrWithDefGw	Notice	IKE Responder: Default LAN gateway is set but peer is not proposing to use this SA as a default route
254	logstrLogIkeProposalOutsideNotNatPub	Notice	IKE Responder: Tunnel terminates outside firewall but proposed local network is not NAT public address
255	logstrLogIkeProposalInsideNotLanDmz	Notice	IKE Responder: Tunnel terminates inside firewall but proposed local network is not inside firewall
410	logstrHashFailed	Notice	Computed hash does not match hash received from peer
411	logstrPayloadMalformed	Notice	Received notify: PAYLOAD_MALFORMED
412	logstrIpsecDeleteRequest	Notice	Received IPSEC SA delete request
413	logstrIkeDeleteRequest	Notice	Received IKE SA delete request
414	logstrInvalidCookies	Notice	Received notify: INVALID_COOKIES
415	logstrResponderLifetime	Notice	Received notify: RESPONDER_LIFETIME
416	logstrNotifyInvalidSpi	Notice	Received notify: INVALID_SPI
417	logstrLogPkiGeneral	Notice	PKI Error:
418	logstrLogIkeProposalBadZeroLocAddr	Notice	IKE Responder: Proposed local network is 0.0.0.0 but SA has no LAN Default Gateway
427	logstrIPsecTunnelStatus	Notice	IPSecTunnel status changed
494	logstrVPNClientLicenseExceeded	Notice	Global VPN Client License Exceeded: Connection denied.
505	logstrBlockQuickModeWithDefaultKeyId	Notice	Blocked Quick Mode for Client using Default Key ID
529	logstrGlobalVPNClientNotAuthorized	Notice	Global VPN Client connection is not allowed. Appliance is not registered.
604	logstrClientVersionNotCompatible	Notice	Global VPN Client version cannot enforce personal firewall. Minimum Version required is 2.1

Info Log Messages

Message ID	Log Event	Priority	Description of Log Event
0	logstrLogHeader1	Info	Log (part
1	logstrLogHeader2	Info	) dumped to email at
2	logstrLogEmailSubject	Info	Log file from SonicWALL
3	logstrAlertEmailSubject	Info	*** Alert from SonicWALL ***
8	logstrLogNewListLoaded	Info	New URL List loaded
9	logstrLogNoNewListAvailable	Info	No new URL List available
10	logstrLogProblemLoadingCheckSettings	Info	Problem loading the URL List; check Filter settings
11	logstrLogProblemLoadingCheckDNS	Info	Problem loading the URL List; check your DNS server
14	logstrWebSiteBlocked	Info	Web site access denied
15	logstrNewsgroupBlocked	Info	Newsgroup access denied
16	logstrWebSiteAccessed	Info	Web site access allowed
17	logstrNewsgroupAccessed	Info	Newsgroup access allowed
18	logstrActiveXBlocked	Info	ActiveX access denied
19	logstrJavaBlocked	Info	Java access denied
20	logstrArchiveBlocked	Info	ActiveX or Java archive access denied
21	logstrCookieRemoved	Info	Cookie removed
22	logstrPingOfDeathBlocked	Info	Ping of death dropped
23	logstrIPSpoofDetected	Info	IP spoof dropped
24	logstrIllegalLanAddressInUse	Info	[not found in tip]
25	logstrPossibleSynFlood	Info	SYN flood attack dropped
26	logstrProbableSynFlood	Info	[not found in tip]
27	logstrLandAttack	Info	Land attack dropped
28	logstrFragmentedPacket	Info	Fragmented packet dropped
36	logstrTCPDropped	Info	TCP connection dropped
37	logstrUDPDropped	Info	UDP packet dropped
38	logstrICMPDropped	Info	ICMP packet dropped
39	logstrPptpDropped	Info	PPTP packet dropped
40	logstrIpsecDropped	Info	IPSec packet dropped
41	logstrUnknownProtocolDropped	Info	Unknown protocol dropped
42	logstrSimultIpsecConnDropped	Info	IPSec packet dropped; waiting for pending IPSec connection

Message ID	Log Event	Priority	Description of Log Event
43	logstrIpsecInterruptErr	Info	IPSec connection interrupt
44	logstrNATCouldntRemap	Info	NAT could not remap incoming packet
45	logstrArpFailure	Info	ARP timeout
46	logstrBroadcastDropped	Info	Broadcast packet dropped
47	logstrNoICMPRedirectSent	Info	No ICMP redirect sent
48	logstrOutOfOrderDropped	Info	Out-of-order command packet dropped
49	logstrDataChannelAddFailed	Info	Failure to add data channel
50	logstrRADecodeFailed	Info	RealAudio decode failure
51	logstrDuplicatePacketDropped	Info	Duplicate packet dropped
52	logstrNoHostTagFound	Info	No HOST tag found in HTTP request
54	logstrCode	Info	Code:
55	logstrType	Info	Type:
56	logstrSource	Info	Source:
57	logstrDestination	Info	Destination:
59	logstrRuleIndex	Info	Rule
60	logstrProxyAccessBlocked	Info	Access to proxy server denied
63	logstrLogICMPTooBig	Info	Received fragmented packet or fragmentation needed
71	logstrSPI	Info	SPI:
72	logstrNetBusDropped	Info	NetBus attack dropped
73	logstrBackOrificeDropped	Info	Back Orifice attack dropped
74	logstrNetSpyDropped	Info	Net Spy attack dropped
75	logstrSub7Dropped	Info	Sub Seven attack dropped
76	logstrRipperDropped	Info	Ripper attack dropped
77	logstrStrikerDropped	Info	Striker attack dropped
78	logstrSennaSpyDropped	Info	Senna Spy attack dropped
79	logstrPriorityDropped	Info	Priority attack dropped
80	logstrIniKillerDropped	Info	Ini Killer attack dropped
81	logstrSmurfDropped	Info	Smurf Amplification attack dropped
82	logstrPortScanPossible	Info	Possible port scan dropped
83	logstrPortScanProbable	Info	Probable port scan dropped
84	logstrCantResolve	Info	Failed to resolve name

Message ID	Log Event	Priority	Description of Log Event
85	logstrLocalRange	Info	local range:
86	logstrRemoteRange	Info	remote range:
96	logstrLogStatusEvent	Info	Status
97	logstrSyslogWebSiteAccessed	Info	#Web site hit
98	logstrSyslogConnectionLogged	Info	Connection Opened
123	logstrAVAccessWithoutAgent	Info	Access attempt from host without Anti-Virus agent installed
124	logstrAVAgentOutOfDate	Info	Anti-Virus agent out-of-date on host
125	logstrAVReceivedAlert	Info	Received AV Alert: %s
126	logstrAVUnused	Info	Unused AV log entry.
127	logstrPppoeStarting	Info	Starting PPPoE discovery
128	logstrPppoeLinkUp	Info	PPPoE LCP Link Up
129	logstrPppoeLinkDown	Info	PPPoE LCP Link Down
130	logstrPppoeLinkFin	Info	PPPoE terminated
131	logstrPppoeNlUp	Info	PPPoE Network Connected
132	logstrPppoeNlDown	Info	PPPoE Network Disconnected
133	logstrPppoePads	Info	PPPoE discovery process complete
134	logstrPppoeChapAuthReq	Info	PPPoE starting CHAP Authentication
135	logstrPppoePapAuthReq	Info	PPPoE starting PAP Authentication
136	logstrPppoeChapAuthFail	Info	PPPoE CHAP Authentication Failed
137	logstrPppoePapAuthFail	Info	PPPoE PAP Authentication Failed
138	logstrWanIpChange	Info	Wan IP Changed
139	logstrXauthSuccess	Info	XAUTH Succeeded with VPN client
140	logstrXauthFailure	Info	XAUTH Failed with VPN client, Authentication failure
141	logstrXauthRadiusTimeout	Info	XAUTH Failed with VPN client, Cannot Contact RADIUS Server
144	logstrHaActivePrimary	Info	Primary firewall has transitioned to Active
145	logstrHaActiveBackup	Info	Backup firewall has transitioned to Active
146	logstrHaIdlePrimary	Info	Primary firewall has transitioned to Idle

Message ID	Log Event	Priority	Description of Log Event
147	logstrHaIdleBackup	Info	Backup firewall has transitioned to Idle
148	logstrHaMissedHeartbeatPrimary	Info	Primary missed heartbeats from Backup
149	logstrHaMissedHeartbeatBackup	Info	Backup missed heartbeats from Primary
150	logstrHaErrorReceivedPrimary	Info	Primary received error/reboot signal from Backup
151	logstrHaErrorReceivedBackup	Info	Backup received error/reboot signal from Primary
152	logstrHaBackupPreempt	Info	Backup firewall being preempted by Primary
153	logstrHaPrimaryPreempt	Info	Primary firewall preempting Backup
154	logstrActiveBackupBackdown	Info	Active Backup detects Active Primary: Backup going Idle
155	logstrHaPrefsImportError	Info	Imported HA hardware ID did not match this firewall
156	logstrHaDiscoveredBackup	Info	Discovered HA Backup Firewall
157	logstrHaSyncedHaPeer	Info	HA Peer Firewall Synchronized
158	logstrHaSyncingError	Info	Error Synchronizing HA Peer Firewall
159	logstrAVExpiredMsg	Info	Received AV Alert: Your SonicWALL Network Anti-Virus subscription has expired. %s
160	logstrHaWrongSrcPrimary	Info	Primary received heartbeat from wrong source
161	logstrHaWrongSrcBackup	Info	Backup received heartbeat from wrong source
162	logstrHaPktError	Info	HA packet processing error
163	logstrHaContentNotMatch	Info	Heartbeat received from incompatible source
165	logstrForbiddenAttDisabled	Info	Forbidden E-Mail attachment disabled
166	logstrPppoeAuthAck	Info	PPPoE PAP Authentication success.
167	logstrPppoeAuthNak	Info	PPPoE PAP Authentication Failed. Please verify PPPoE username and password
168	logstrPppoeTrafficTimeout	Info	Disconnecting PPPoE due to traffic timeout

Message ID	Log Event	Priority	Description of Log Event
169	logstrPppoeLcpUnacked	Info	No response from ISP Disconnecting PPPoE.
170	logstrBackupActivePreempt	Info	Backup going Active in preempt mode after reboot
171	logstrVpn	Info	VPN Log
172	logstrVpnDebug	Info	VPN Log Debug
173	logstrLanTCPDenied	Info	TCP connection from LAN denied
174	logstrLanUDPDenied	Info	UDP packet from LAN dropped
175	logstrLanICMPDenied	Info	ICMP packet from LAN dropped
176	logstrLanPktRcvd	Info	[not found in tip]
177	logstrTcpFinScanDropped	Info	Probable TCP FIN scan dropped
178	logstrTcpXmasScanDropped	Info	Probable TCP XMAS scan dropped
179	logstrTcpNullScanDropped	Info	Probable TCP NULL scan dropped
181	logstrTcpFinDropped	Info	TCP FIN packet dropped
182	logstrVpnRcvdPmtuIcmp	Info	Received a path MTU icmp message from router/gateway
183	logstrCflUpdateApplianceNotRegistered	Info	Problem loading the URL List; Appliance not registered.
184	logstrCflUpdateSubscriptionExpired	Info	Problem loading the URL List; Subscription expired.
185	logstrCflUpdateErrorTransient	Info	Problem loading the URL List; Try loading it again.
186	logstrCflUpdateErrorTransientAuto	Info	Problem loading the URL List; Retrying later.
187	logstrCflUpdateErrorInternal	Info	Problem loading the URL List; Flash write failure.
188	logstrPmtuIcmp	Info	Received a path MTU icmp message from router/gateway
189	logstrMTU	Info	MTU:
190	logstrCflApplianceCflExpired	Info	The loaded content URL List has expired.
191	logstrHaSetError	Info	Error setting the IP address of the backup, please manually set to backup LAN IP
192	logstrHaSyncError	Info	Error updating HA peer configuration
193	logstrFakeCertFound	Info	Fraudulent Microsoft certificate found; access denied
194	logstrTCPStatSYN	Info	VPN TCP SYN

Message ID	Log Event	Priority	Description of Log Event
195	logstrTCPStatFIN	Info	VPN TCP FIN
196	logstrTCPStatPSH	Info	VPN TCP PSH
197	logstrCflSubscriptionExpiredEmailSubject	Info	Content filter subscription expired.
201	logstrL2tpTunnelStarting	Info	L2TP Tunnel Negotiation Started
202	logstrL2tpSessionStarting	Info	L2TP Session Negotiation Started
203	logstrL2tpMaxReTransExceed	Info	L2TP Max Retransmission Exceeded
204	logstrL2tpTunnelFinished	Info	L2TP Tunnel Established
205	logstrL2tpTunnelDisconRem	Info	L2TP Tunnel Disconnect from Remote
206	logstrL2tpSessionSuccess	Info	L2TP Session Established
207	logstrL2tpCallDisConnRem	Info	L2TP Session Disconnect from Remote
208	logstrL2tpPPPStarts	Info	L2TP PPP Negotiation Started
209	logstrL2tpLCPDown	Info	L2TP LCP Down
210	logstrL2tpPPPUp	Info	L2TP PPP Session Up
211	logstrL2tpNetDown	Info	L2TP PPP Down
212	logstrL2tpPPPAuthFail	Info	L2TP PPP Authentication Failed
213	logstrL2toLCPUp	Info	L2TP LCP Up
214	logStrL2tpUserDiscon	Info	L2TP Disconnect Initiated by the User
215	logstrL2tpTrafficTimeout	Info	Disconnecting L2TP Tunnel due to traffic timeout
216	logStrL2tpUserCon	Info	L2TP Connect Initiated by the User
217	logStrL2tpPPPDown	Info	L2TP PPP link down
218	logstrPrimaryLinkDownBackoff	Info	Primary WAN link down, Primary going Idle
219	logstrBackupLinkDown	Info	Backup WAN link down, Primary going Active
220	logstrPrimaryLinkDown	Info	Primary WAN link down, Backup going Active
221	logstrPrimaryLinkBackUp	Info	Primary WAN link up, preempting Backup
243	logstrUserLoginRadiusFail	Info	User login denied - RADIUS authentication failure
244	logstrUserLoginRadiusTimeout	Info	User login denied - RADIUS server timeout

Message ID	Log Event	Priority	Description of Log Event
245	logstrUserLoginRadiusError	Info	User login denied - RADIUS configuration error
246	logstrUserLoginFromWrongLocation	Info	User login denied - User has no privileges for login from that location
248	logstrForbiddenAttDeleted	Info	Forbidden E-Mail attachment deleted
267	logstrTcpXmasTreeDropped	Info	TCP Xmas Tree dropped
268	logstrCflAutoBroken	Info	CFL auto-download disabled, time problem detected
281	logstrDialing	Info	PPP Dial-Up: Dialing: %s
282	logstrDialNoDialtone	Info	PPP Dial-Up: No dialtone detected - check phone-line connection
283	logstrDialNoCarrier	Info	PPP Dial-Up: No link carrier detected - check phone number
284	logstrDialBusy	Info	PPP Dial-Up: Dialed number is busy
285	logstrDialNoAnswer	Info	PPP Dial-Up: Dialed number did not answer
286	logstrDialStartingPpp	Info	PPP Dial-Up: Connected at %s bps - starting PPP
287	logstrDialFailure	Info	PPP Dial-Up: Unknown dialing failure
288	logstrDialDisconnected	Info	PPP Dial-Up: Link carrier lost
289	logstrPppAuthOk	Info	PPP: Authentication successful
290	logstrPppPapAuthFailed	Info	PPP: PAP Authentication failed - check username / password
291	logstrPppChapAuthFailed	Info	PPP: CHAP authentication failed - check username / password
292	logstrPppMschapAuthFailed	Info	PPP: MS-CHAP authentication failed - check username / password
293	logstrPppMSChapStarting	Info	PPP: Starting MS-CHAP authentication
294	logstrPppChapStarting	Info	PPP: Starting CHAP authentication
295	logstrPppPapStarting	Info	PPP: Starting PAP authentication
296	logstrPppduNegotiationFailed	Info	PPP Dial-Up: PPP negotiation failed - disconnecting
297	logstrPppduIdleExceeded	Info	PPP Dial-Up: Idle time limit exceeded - disconnecting

Message ID	Log Event	Priority	Description of Log Event
298	logstrPppduIpcpFailed	Info	PPP Dial-Up: Failed to get IP address
299	logstrPppduIpcpUp	Info	PPP Dial-Up: Received new IP address
300	logstrPppduPppEst	Info	PPP Dial-Up: PPP link established
301	logstrPppduLinkDown	Info	PPP Dial-Up: PPP link down
302	logstrPppduLinkClosing	Info	PPP Dial-Up: Shutting down link
303	logstrDialModemStr	Info	PPP Dial-Up: Initialization : %s
304	logstrPppduUserDisconnect	Info	PPP Dial-Up: User requested disconnect
305	logstrPppduUserConnect	Info	PPP Dial-Up: User requested connect
306	logstrDialCanceled	Info	PPP Dial-Up: Connect request canceled
308	logstrLogL2TPsTunnelUp	Info	L2TP Server: L2TP Tunnel Established.
309	logstrLogL2TPsSessionUp	Info	L2TP Server: L2TP Session Established.
310	logstrLogL2TPsPPPUp	Info	L2TP Server: L2TP PPP Session Established.
311	logstrLogL2TPsRadAuthFailure	Info	L2TP Server: Radius reports Authentication Failure
312	logstrLogL2TPsLocalAuthFailure	Info	L2TP Server: Local Authentication Failure
313	logstrLogL2TPsRadIPFailure	Info	L2TP Server: Radius server not assigned IP address
314	logstrLogL2TPsLocalIPFailure	Info	L2TP Server: No IP address available in the Local IP Pool
315	logstrLogL2TPsTunnelDiscRemote	Info	L2TP Server: L2TP Tunnel Disconnect from the Remote.
316	logsstrLogL2TPsSessionDiscRemote	Info	L2TP Server: L2TP Session Disconnect from the Remote.
317	logstrLogL2TpsPPPTermFromRemote	Info	L2TP Server: L2TP Remote terminated the PPP session
318	logstrLogL2tpsLocalAuthSuccess	Info	L2TP Server: Local Authentication Success.
319	logstrLogL2tpsRadAuthSuccess	Info	L2TP Server: Radius Authentication Success
320	logstrLogL2tpsKeepAliveFailure	Info	L2TP Server: Keep alive Failure. Closing Tunnel

Message ID	Log Event	Priority	Description of Log Event
321	logstrPppduNeedManualAction	Info	PPP Dial-Up: Manual intervention needed. Check Primary Profile or Profile details
322	logstrWfoManualProfile	Info	PPP Dial-Up: Trying to failover but Primary Profile is manual
323	logstrPppduAutoDetect	Info	PPP Dial-Up: Startup without Ethernet cable, will try to dial on outbound traffic
324	logstrPppduStartBy	Info	PPP Dial-Up: Dial initiated by %s
327	logstrPppduMaxConnExceeded	Info	PPP Dial-Up: Maximum connection time exceeded - disconnecting
330	logstrPppduVpnDisabled	Info	PPP Dial-Up: The profile in use disabled VPN networking.
331	logstrPppduVpnEnabled	Info	PPP Dial-Up: VPN networking restored.
334	logstrLogL2TPsCDNFromRemote	Info	L2TP Server: Call Disconnect from Remote.
335	logstrLogL2TPsStopCCNFromRemote	Info	L2TP Server: Tunnel Disconnect from Remote.
336	logstrLogL2TPsDeleteTunnel	Info	L2TP Server: Deleting the Tunnel
337	logstrLogL2TPsDeleteSession	Info	L2TP Server: Deleting the L2TP active Session
338	logstrLogL2TPsRetransExceeded	Info	L2TP Server: Retransmission Timeout, Deleting the Tunnel
339	logstrNatOverwrite	Info	NAT translated packet exceeds size limit, packet dropped
343	logstrL2TPsNoPrivForL2TPRadius	Info	L2TP Server: Access from L2TP VPN Client Privilege not enabled for Radius Users.
344	logstrL2TPsNoPrivForL2TPLocal	Info	L2TP Server: User Name authentication Failure locally.
347	logstrPktDropInClear	Info	Port configured to receive IPSEC ONLY. Drop packet received in the clear.
371	logstrClientPolicyProvisioning	Info	VPN Client Policy Provisioning
372	logstrLogInitiatorIkeProposalOK	Info	IKE Initiator: Accepting IPSec proposal (Phase 2)
373	logstrRespAMPhase1Complete	Info	IKE Responder: Aggressive Mode complete (Phase 1)
375	logstrPptpCtrlConnStarting	Info	PPTP Control Connection Negotiation Started
376	logstrPptpSessionStarting	Info	PPTP Session Negotiation Started

Message ID	Log Event	Priority	Description of Log Event
377	logstrPptpMaxReTransExceed	Info	PPTP Max Retransmission Exceeded
378	logstrPptpCtrlConnEstablished	Info	PPTP Control Connection Established
379	logstrPptpTunnelDisconRem	Info	PPTP Tunnel Disconnect from Remote
380	logstrPptpSessionSuccess	Info	PPTP Session Established
381	logstrPptpCallDisConnRem	Info	PPTP Session Disconnect from Remote
382	logstrPptpPPPStarts	Info	PPTP PPP Negotiation Started
383	logstrPptpLCPDown	Info	PPTP LCP Down
384	logstrPptpPPPUp	Info	PPTP PPP Session Up
385	logstrPptpNetDown	Info	PPTP PPP Down
386	logstrPptpPPPAuthFail	Info	PPTP PPP Authentication Failed
387	logstrPptpLCPUp	Info	PPTP LCP Up
388	logStrPptpUserDiscon	Info	PPTP Disconnect Initiated by the User
389	logstrPptpTrafficTimeout	Info	Disconnecting PPTP Tunnel due to traffic timeout
390	logStrPptpUserCon	Info	PPTP Connect Initiated by the User
391	logStrPptpPPPDown	Info	PPTP PPP link down
392	logstrPptpChapAuthReq	Info	PPTP starting CHAP Authentication
393	logstrPptpPapAuthReq	Info	PPTP starting PAP Authentication
394	logstrPptpChapAuthFail	Info	PPTP CHAP Authentication Failed. Please verify PPTP username and password
395	logstrPptpPapAuthFail	Info	PPTP PAP Authentication Failed
396	logstrPptpAuthAck	Info	PPTP PAP Authentication success.
397	logstrPptpAuthNak	Info	PPTP PAP Authentication Failed. Please verify PPTP username and password
398	logstrPptpPPPlinkUp	Info	PPTP PPP Link Up
399	logstrPptpPPPlinkDown	Info	PPTP PPP Link down
400	logstrPptpPPPlinkFinished	Info	PPTP PPP Link Finished
401	logstrNoProposalChosen	Info	IKE Initiator: Received notify. NO_PROPOSAL_CHOSEN

Message ID	Log Event	Priority	Description of Log Event
402	logstrLogIkeProposalReject	Info	IKE Responder: IKE proposal does not match (Phase 1)
403	logstrLogIkeAbort	Info	IKE negotiation aborted due to timeout
404	logstrDecryptFailedWithPsk	Info	Failed payload verification after decryption. Possible preshared key mismatch
405	logstrVerifyAfterDecryptFailed	Info	Failed payload verification after decryption
406	logstrDropDuplicatePacket	Info	Received packet retransmission. Drop duplicate packet
407	logstrSADisabled	Info	SA is disabled. Check VPN SA settings
408	logstrAvEnforcedLicensesExceeded	Info	Anti-Virus Licenses Exceeded
409	logstrAuthFailed	Info	Received notify: ISAKMP_AUTH_FAILED
419	logstrLanRipModeOff	Info	RIP disabled on interface %s
420	logstrLanRipModeV1	Info	RIPv1 enabled on interface %s
421	logstrLanRipModeV2	Info	RIPv2 enabled on interface %s
422	logstrLanRipModeV2C	Info	RIPv2 compatibility (broadcast) mode enabled on interface %s
423	logstrDmzRipModeOff	Info	RIP disabled on DMZ interface
424	logstrDmzRipModeV1	Info	RIPv1 enabled on DMZ interface
425	logstrDmzRipModeV2	Info	RIPv2 enabled on DMZ interface
426	logstrDmzRipModeV2C	Info	RIPv2 compatibility (broadcast) mode enabled on DMZ interface
428	logstrDropSrcRtPkt	Info	Source routed IP packet dropped
429	logstrPptpDisconEchoRq	Info	No response from server to Echo Requests, disconnecting PPTP Tunnel
430	logstrPptpDisconCtrlConnRq	Info	No response from PPTP server to control connection requests
431	logstrPptpDisconCallRq	Info	No response from PPTP server to call requests
432	logstrPptpDisconCtrlConnRej	Info	PPTP server rejected control connection
433	logstrPptpDisconCallRej	Info	PPTP server rejected the call request
437	logstrDroppedMsgPartial	Info	E-Mail fragment dropped
440	logstrRuleAdded	Info	Access Rule added

Message ID	Log Event	Priority	Description of Log Event
441	logstrRuleModified	Info	Access Rule modified
442	logstrRuleDeleted	Info	Access Rule deleted
443	logstrRuleTableDefaulted	Info	Access Rules restored to defaults
444	logstrPptpServerDown	Info	PPTP Server is not responding, check if the server is UP and running.
446	logstrFtpPasvRspSpoof	Info	FTP: PASV response spoof attack dropped
471	logstrVpnClean	Info	VPN Cleanup: Dynamic network settings change
481	logstrPppduNoPeerIp	Info	PPP Dial-Up: No peer IP address from Dial-Up ISP, local and remote IPs will be the same
482	logstrAVExpirationWarningMsg	Info	Received AV Alert: Your SonicWALL Network Anti-Virus subscription will expire in 7 days. %s
485	logstrCategory	Info	Category:
489	logstrCFSExpirationWarningMsg	Info	Received CFS Alert: Your SonicWALL Content Filtering subscription will expire in 7 days.
490	logstrCFSExpirationMsg	Info	Received CFS Alert: Your SonicWALL Content Filtering subscription has expired.
491	logstrMafiaExpirationWarningMsg	Info	Received E-Mail Filter Alert: Your SonicWALL E-Mail Filtering subscription will expire in 7 days.
492	logstrMafiaExpirationMsg	Info	Received E-Mail Filter Alert: Your SonicWALL E-Mail Filtering subscription has expired.
496	logstrDeaRegInc	Info	SonicWALL Registration Update Needed: Restore your existing security service subscriptions
499	logstrPPPPoENotReady	Info	PPPoE enabled but not ready
500	logstrL2TPNotReady	Info	L2TP enabled but not ready
501	logstrPPTPNotReady	Info	PPTP enabled but not ready
503	logstrVPNDisDialup	Info	VPN disabled for active dial up
522	logstrMalformedIpPacket	Info	Malformed IP packet dropped.
523	logstrNoMatchICMPDropped	Info	ICMP packet dropped
524	logstrWebAccessRequestDropped	Info	Web access request dropped
525	logstrProtocol	Info	Protocol:

Message ID	Log Event	Priority	Description of Log Event
526	logstrWebAccessRequestRcvd	Info	Web management request allowed
527	logstrFtpPortBounceAttack	Info	FTP: PORT bounce attack dropped.
528	logstrFtpPasvBounceAttack	Info	FTP: PASV response bounce attack dropped.
537	logstrSyslogCloseLogged	Info	Connection Closed
538	logstrFtpDataPort	Info	FTP: Data connection from non default port dropped
552	logstrWanRipModeOff	Info	RIP disabled on WAN interface
553	logstrWanRipModeV1	Info	RIPv1 enabled on WAN interface
554	logstrWanRipModeV2	Info	RIPv2 enabled on WAN interface
555	logstrWanRipModeV2C	Info	RIPv2 compatibility (broadcast) mode enabled on WAN interface
571	logStrRipWanOn	Info	RIP Broadcasts for LAN Network %s are being broadcast over dialup-connection
580	logstrTcpSynFinDropped	Info	TCP Syn/Fin packet dropped
590	logstrLanIpDenied	Info	IP type %s packet dropped
591	logstrMaxFailedDials	Info	Maximum sequential failed dial attempts (10) to a single dial-up number: %s
592	logstr30MinDialDelay	Info	Regulatory requirements prohibit %s from being re-dialed for 30 minutes
593	logstrReceivedPADO	Info	Received PPPoE Active Discovery Offer
594	logstrReceivedPADS	Info	Received PPPoE Active Discovery Session_confirmation
595	logstrSendingPADR	Info	Sending PPPoE Active Discovery Request
596	logstrPPTPDecodeFailed	Info	PPTP decode failure
597	logstrICMPAllowed	Info	ICMP packet allowed
598	logstrLanICMPAllowed	Info	ICMP packet from LAN allowed
602	logstrDNSAllowed	Info	DNS packet allowed
603	logstrLogProblemAddingL2tpIpPool	Info	Adding L2TP IP pool Address object Failed.
606	logstrSpankAttackDropped	Info	Spank attack multicast packet dropped
608	logstrIDPDetectionAlert	Info	IPS Detection Alert: %s

Message ID	Log Event	Priority	Description of Log Event
609	logstrIDPPreventionAlert	Info	IPS Prevention Alert: %s
614	logstrIDPExpiredMsg	Info	Received IPS Alert: Your SonicWALL Intrusion Prevention (IDP) subscription has expired.
622	logstrVoipCallConnect	Info	VoIP Call Connected
623	logstrVoipCallDisconnect	Info	VoIP Call Disconnected
624	logstrVoipAdmissionReject	Info	H.323/RAS Admission Reject
625	logstrVoipAdmissionConfirm	Info	H.323/RAS Admission Confirm
626	logstrVoipAdmissionRequest	Info	H.323/RAS Admission Request
627	logstrVoipBandwidthReject	Info	H.323/RAS Bandwidth Reject
628	logstrVoipDisengageConfirm	Info	H.323/RAS Disengage Confirm
629	logstrVoipGatekeeperReject	Info	H.323/RAS Gatekeeper Reject
630	logstrVoipLocationConfirm	Info	H.323/RAS Location Confirm
631	logstrVoipLocationReject	Info	H.323/RAS Location Reject
632	logstrVoipRegistrationReject	Info	H.323/RAS Registration Reject
633	logstrVoipSetup	Info	H.323/H.225 Setup
634	logstrVoipConnect	Info	H.323/H.225 Connect
635	logstrVoipAddress	Info	H.323/H.245 Address
636	logstrVoipEndSession	Info	H.323/H.245 End Session
637	logstrVoipEndpointAdded	Info	H.323 %s Endpoint added
638	logstrVoipEndpointRemoved	Info	H.323 %s Endpoint removed
639	logstrVoipSpare18	Info	unused/spare
640	logstrVoipSpare19	Info	unused/spare
641	logstrVoipSpare20	Info	unused/spare
642	logstrVoipSpare21	Info	unused/spare
643	logstrVoipSpare22	Info	unused/spare
644	logstrVoipSpare23	Info	unused/spare
645	logstrVoipSpare24	Info	unused/spare
646	logstrVoipSpare25	Info	unused/spare
647	logstrVoipSpare26	Info	unused/spare
648	logstrVoipSpare27	Info	unused/spare
649	logstrVoipSpare28	Info	unused/spare
650	logstrVoipSpare29	Info	unused/spare
651	logstrVoipSpare30	Info	unused/spare

Message ID	Log Event	Priority	Description of Log Event
652	logstrVoipSpare31	Info	unused/spare
653	logstrVoipSpare32	Info	unused/spare
655	logstrLogSyslogDataRateExceeded	Info	Maximum syslog data per second threshold exceeded
656	logstrLogSpare3	Info	unused/spare
657	logstrLogSpare4	Info	unused/spare

Debug Log Messages

Message ID	Log Event	Priority	Description of Log Event
99	logstrDHCPCRetransDiscover	Debug	Retransmitting DHCP DISCOVER.
100	logstrDHCPCRetransRequestRequest	Debug	Retransmitting DHCP REQUEST (Requesting).
101	logstrDHCPCRetransRequestRenew	Debug	Retransmitting DHCP REQUEST (Renewing).
102	logstrDHCPCRetransRequestRebind	Debug	Retransmitting DHCP REQUEST (Rebinding).
103	logstrDHCPCRetransRequestReboot	Debug	Retransmitting DHCP REQUEST (Rebooting).
104	logstrDHCPCRetransRequestVerify	Debug	Retransmitting DHCP REQUEST (Verifying).
105	logstrDHCPCSendDiscover	Debug	Sending DHCP DISCOVER.
106	logstrDHCPCNoOffers	Debug	DHCP Server not available. Did not get any DHCP OFFER.
107	logstrDHCPCGotOffer	Debug	Got DHCP OFFER. Selecting.
108	logstrDHCPCSelecting	Debug	Sending DHCP REQUEST.
109	logstrDHCPCRequestFailed	Debug	DHCP Client did not get DHCP ACK.
110	logstrDHCPCRequestNAK	Debug	DHCP Client got NACK.
111	logstrDHCPCRequestACK	Debug	DHCP Client got ACK from server.
112	logstrDHCPCRequestDecline	Debug	DHCP Client is declining address offered by the server.
113	logstrDHCPCBoundRebind	Debug	DHCP Client sending REQUEST and going to REBIND state.
262	logstrAdminSessInactivity	Debug	Administrator logged out - inactivity timer expired
263	logstrUserLogout	Debug	User logged out
264	logstrUserSessTimeout	Debug	User logged out - max session time exceeded
265	logstrUserSessInactivity	Debug	User logged out - inactivity timer expired
328	logstrAdminNameChanged	Debug	Administrator name changed
329	logstrUserLoginLockout	Debug	User login failure rate exceeded - logins from user IP address denied
359	logstrCryptFipsErrorState	Debug	Entering FIPS ERROR state
360	logstrCryptDesTestFailed	Debug	Crypto DES test failed
361	logstrCryptDhTestFailed	Debug	Crypto DH test failed
362	logstrCryptHmacMD5TestFailed	Debug	Crypto Hmac-MD5 fest failed
363	logstrCryptHmacSha1TestFailed	Debug	Crypto Hmac-Sha1 test failed

Message ID	Log Event	Priority	Description of Log Event
364	logstrCryptRsaTestFailed	Debug	Crypto RSA test failed
365	logstrCryptSha1TestFailed	Debug	Crypto Sha1 test failed
366	logstrCryptHwDesTestFailed	Debug	Crypto hardware DES test failed
367	logstrCryptHw3DesTestFailed	Debug	Crypto Hardware 3Des test failed
368	logstrCryptHwDesShaTestFailed	Debug	Crypto Hardware DES with SHA test failed
369	logstrCryptHw3DesShaTestFailed	Debug	Crypto Hardware 3DES with SHA test failed
370	logstrCryptMd5TestFailed	Debug	Crypto MD5 test failed
438	logstrUserLoginLockoutExpire	Debug	Locked-out user logins allowed - lockout period expired
439	logstrUserLoginLockoutClear	Debug	Locked-out user logins allowed by administrator
486	logstrWlanNoGuestPrivilege	Debug	User login denied - User has no privileges for WLAN guest service
497	logstrFipsChangeState2Error	Debug	Entering FIPS Error State.
506	logStrVpnDisabled	Debug	VPN disabled by administrator
507	logStrVpnEnabled	Debug	VPN enabled by administrator
508	logStrWlanDisabled	Debug	WLAN disabled by administrator
509	logStrWlanEnabled	Debug	WLAN enabled by administrator
510	logStrWiFiSecDisabled	Debug	WiFiSec Enforcement disabled by administrator
511	logStrWiFiSecEnabled	Debug	WiFiSec Enforcement enabled by administrator
512	logStrMacFilterListEnabled	Debug	Wireless MAC Filter List enabled by administrator
513	logStrMacFilterListDisabled	Debug	Wireless MAC Filter List disabled by administrator
514	logstrPPPoEUserChanged	Debug	PPPoE user name changed by Administrator
515	logstrPPPoEPasswordChanged	Debug	PPPoE password changed by Administrator
520	logstrAdminLogoutFromCLI	Debug	CLI administrator logged out
549	logstrWlanGuestLimit	Debug	User login failed - User has no privileges for wlan guest service
550	logstrWlanSessionTimeout	Debug	Wlan Guest Session Timeout
551	logstrWlanAccountTimeout	Debug	Wlan Guest Account Timeout
557	logstrWlanGuestAlreadyLoggedIn	Debug	Guest login denied. Guest '%s' is already logged in. Please try again later.
558	logstrWlanGuestCreated	Debug	Guest account '%s' created
559	logstrWlanGuestDeleted	Debug	Guest account '%s' deleted
560	logstrWlanGuestDisabled	Debug	Guest account '%s' disabled
561	logstrWlanGuestReEnabled	Debug	Guest account '%s' re-enabled
562	logstrWlanGuestPruned	Debug	Guest account '%s' pruned
563	logstrWlanGuestReGenerated	Debug	Guest account '%s' re-generated
564	logstrWlanIdleTimeout	Debug	Wlan Guest Idle Timeout
583	logstrUserLoginDisabled	Debug	User login disabled from %s
610	logstrCryptHwAesTestFailed	Debug	Crypto Hardware AES test failed

Message ID	Log Event	Priority	Description of Log Event
618	logstrBootpCentralAck	Debug	BOOTP server response relayed to remote device
619	logstrBootpReplyConflict	Debug	BOOTP Client IP address on LAN conflicts with remote device IP, deleting IP address from remote table
620	logstrBootpRemoteAck	Debug	BOOTP reply relayed to local device
621	logstrBootpRequestMessage	Debug	BOOTP Request received from remote device

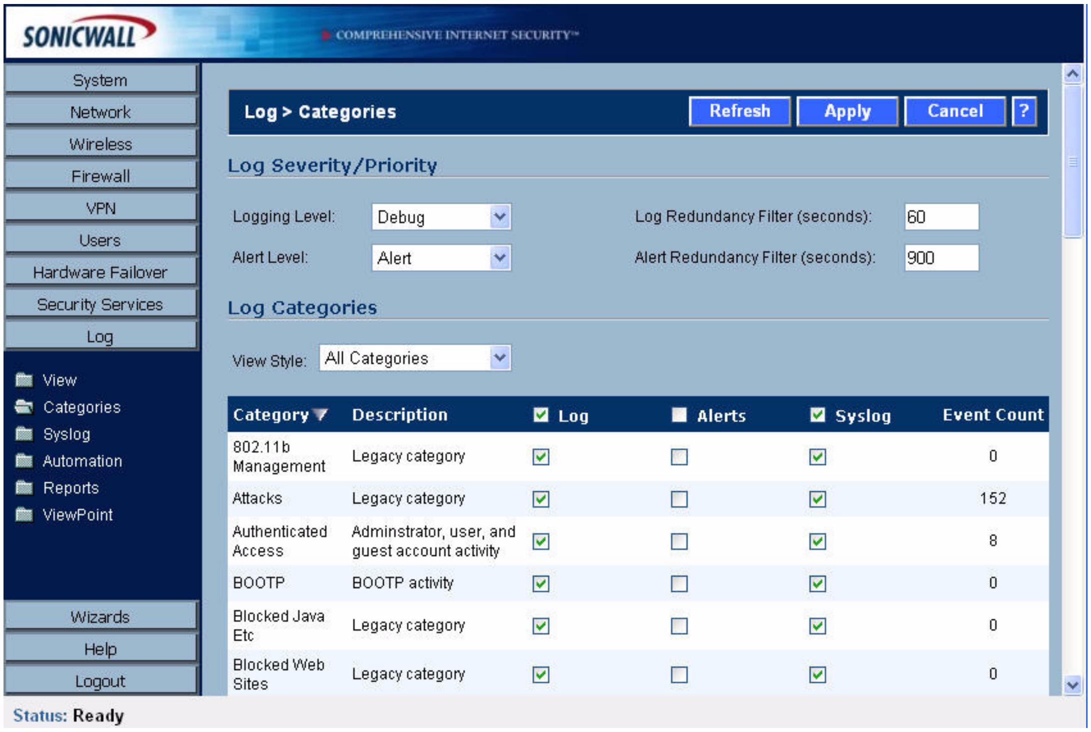
CHAPTER 43

Configuring Log Categories

Log > Categories

This chapter provides configuration tasks to enable you to categorize and customize the logging functions on your SonicWALL security appliance for troubleshooting and diagnostics.

Note: You can extend your SonicWALL security appliance log reporting capabilities by using SonicWALL ViewPoint. ViewPoint is a web-based graphical reporting tool for detailed and comprehensive reports. For more information on the SonicWALL ViewPoint reporting tool, refer to www.sonicwall.com.


SONICWALL
COMPREHENSIVE INTERNET SECURITY
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
View
Categories
Syslog
Automation
Reports
ViewPoint
Wizards
Help
Logout
Refresh
Apply
Cancel
?

Log > Categories

Log Severity/Priority

Logging Level: Debug

Alert Level: Alert

Log Redundancy Filter (seconds): 60

Alert Redundancy Filter (seconds): 900

Log Categories

View Style: All Categories

Category	Description	☑ Log	☐ Alerts	☑ Syslog	Event Count
802.11b Management	Legacy category	☑	☐	☑	0
Attacks	Legacy category	☑	☐	☑	152
Authenticated Access	Adminstrator, user, and guest account activity	☑	☐	☑	8
BOOTP	BOOTP activity	☑	☐	☑	0
Blocked Java Etc	Legacy category	☑	☐	☑	0
Blocked Web Sites	Legacy category	☑	☐	☑	0

Status: Ready

Log Priority

This section provides information on configuring the level of priority log messages are captured and corresponding alert messages are sent through e-mail for notification.

Logging Level

The **Logging Level** control filters events by priority. Events of equal of greater priority are passed, and events of lower priority are dropped. The **Logging Level** menu includes the following priority scale items from highest to lowest priority:

- **Emergency** (highest priority)
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debug** (lowest priority)

Alert Level

The **Alert Level** control determines how E-mail Alerts are sent. An event of equal or greater priority causes an E-mail alert to be issued. Lower priority events do not cause an alert to be sent. Events are pre-filtered by the **Logging Level** control, so if the **Logging Level** control is set to a higher priority than that of the **Alert Level** control, only alerts at the **Logging Level** or higher are sent. Alert levels include:

- **Emergency** (highest priority)
- **Alert**
- **Critical**
- **Error** (lowest priority)
- **None** (disables e-mail alerts)

Log Redundancy Filter

The **Log Redundancy Filter** allows you to define the time in seconds that the same attack is logged on the **Log > View** page as a single entry in the SonicWALL log. Various attacks are often rapidly repeated, which can quickly fill up a log if each attack is logged. The Log Redundancy Filter has a default setting of 60 seconds.

Alert Redundancy Filter

The **Alert Redundancy Filter** allows you to define the time in seconds that the same attack is logged on the **Log > View** page as a single entry in the SonicWALL log before an alert is issued. The Alert Redundancy Filter has a default setting of 900 seconds.

Log Categories

SonicWALL security appliances provide automatic attack protection against well known exploits. The majority of these *legacy attacks* were identified by telltale IP or TCP/UDP characteristics, and recognition was limited to a set of fixed layer 3 and layer 4 values. As the breadth and sophistication of attacks evolved, it's become essential to dig deeper into the traffic, and to develop the sort of adaptability that could keep pace with the new threats.

All SonicWALL security appliances, even those running SonicWALL IPS, continue to recognize these legacy port and protocol types of attacks. The current behavior on all SonicWALL security appliances devices is to automatically and holistically prevent these legacy attacks, meaning that it is not possible to disable prevention of these attacks either individually or globally.

SonicWALL security appliances now include an expanded list of attack categories that can be logged.

The **View Style** menu provides the following three log category views:

- **All Categories** - Displays both **Legacy Categories** and **Expanded Categories**.
- **Legacy Categories** - Displays log categories carried over from earlier SonicWALL log event categories.
- **Expanded Categories** - Displays the expanded listing of categories that includes the older Legacy Categories log events rearranged into the new structure.

All Categories

Displays both the **Legacy Categories** and **Expanded Categories** items from the **View Style** menu.

Legacy Categories

Legacy Categories represent the older log event categories that has been replaced with the **Expanded Categories** listing. The **Legacy Categories** are preserved for use in Syslog messages.

- **802.11b Management** - Logs WLAN IEEE 802.11b connections.
- **Attacks** - Logs messages showing Denial of Service attacks, such as SYN Flood, Ping of Death, and IP spoofing.
- **Blocked Java, etc**. - Logs Java, ActiveX, and Cookies blocked by the SonicWALL security appliance.
- **Blocked Web Sites** - Logs Web sites or newsgroups blocked by the Content Filter List or by customized filtering.
- **Denied LAN IP** - Logs all LAN IP addresses denied by the SonicWALL security appliance.
- **Dropped ICMP** - Logs blocked incoming ICMP packets.
- **Dropped TCP** - Logs blocked incoming TCP connections.
- **Dropped UDP** - Logs blocked incoming UDP packets.
- **Network Debug** - Logs NetBIOS broadcasts, ARP resolution problems, and NAT resolution problems. Also, detailed messages for VPN connections are displayed to assist the network administrator with troubleshooting problems with active VPN tunnels. **Network Debug** information is intended for experienced network administrators.
- **System Environment** - Logs physical unit events such as fan failure or power disruption.
- **System Errors** - Logs problems with DNS or e-mail.
- **System Maintenance** - Logs general system activity, such as system activations.
- **User Activity** - Logs successful and unsuccessful log in attempts.
- **VPN Tunnel Status** - Logs status information on VPN tunnels.

Expanded Categories

Expanded Categories includes new functional categories that replace the older **Legacy Categories**, but the older **Legacy Categories** events are included in a rearranged format. The Expanded Categories with descriptions are listed in the **Log Categories** table.

Managing Log Categories

The **Log Categories** table displays log category information organized into the following columns:

- **Category** - Displays log category name.
- **Description** - Provides description of the log category activity type.
- **Log** - Provides checkbox for enabling/disabling the display of the log events in on the **Log > View** page.
- **Alerts** - Provides checkbox for enabling/disabling the sending of alerts for the category.
- **Syslog** - Provides checkbox for enabling/disabling the capture of the log events into the SonicWALL security appliance Syslog.
- **Event Count** - Displays the number of events for that category. Clicking the **Refresh** button updates these numbers.

You can sort the log categories in the **Log Categories** table by clicking on the column header. For example, clicking on the **Category** header sorts the log categories in descending order from the default ascending order. An up or down arrow to the left of the column name indicates whether the column is assorted in ascending or descending order.

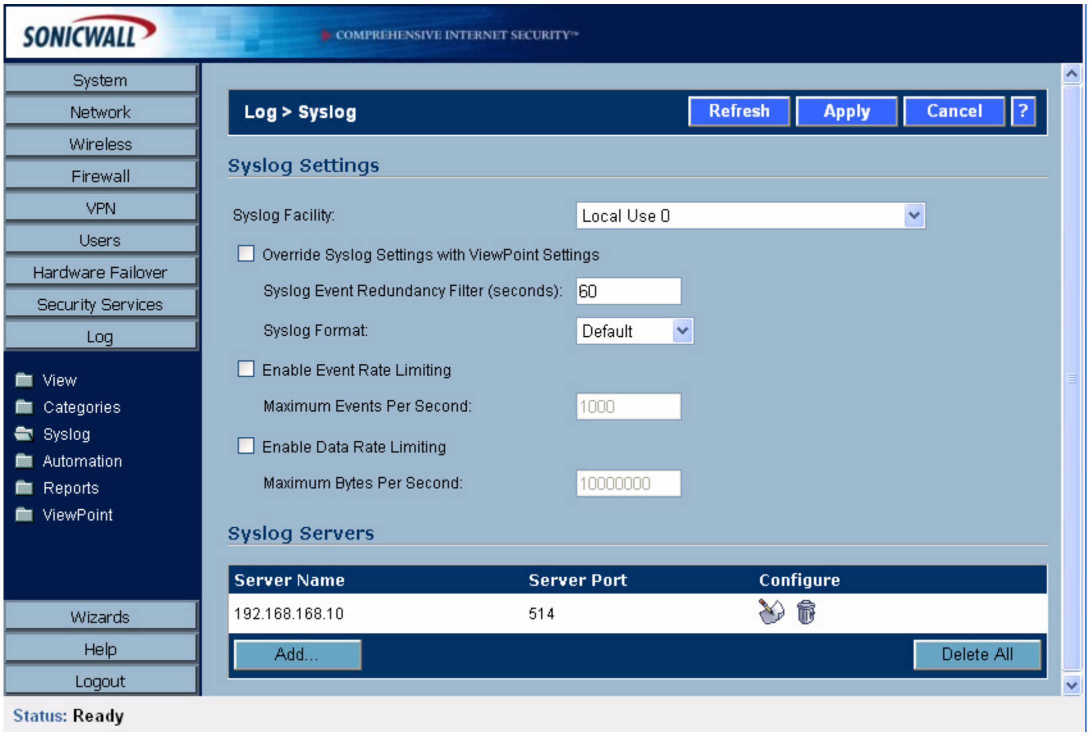
You can enable or disable **Log**, **Alerts**, and **Syslog** on a category by category basis by clicking on the check box for the category in the table. You can enable or disable **Log**, **Alerts**, and **Syslog** for all categories by clicking the checkbox on the column header.

CHAPTER 44

Configuring Syslog Settings

Log > Syslog

In addition to the standard event log, the SonicWALL security appliance can send a detailed log to an external Syslog server. The SonicWALL Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. The SonicWALL Syslog support requires an external server running a Syslog daemon on UDP Port 514. Syslog Analyzers such as SonicWALL ViewPoint or WebTrends Firewall Suite can be used to sort, analyze, and graph the Syslog data. Messages from the SonicWALL security appliance are then sent to the server(s). Up to three Syslog server IP addresses can be added.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
View
Categories
Syslog
Automation
Reports
ViewPoint
Wizards
Help
Logout
Log > Syslog
Refresh
Apply
Cancel
?
Add...
Delete All

Syslog Settings

Syslog Facility: Local Use 0

☐ Override Syslog Settings with ViewPoint Settings

Syslog Event Redundancy Filter (seconds): 60

Syslog Format: Default

☐ Enable Event Rate Limiting

Maximum Events Per Second: 1000

☐ Enable Data Rate Limiting

Maximum Bytes Per Second: 10000000

Syslog Servers

Server Name	Server Port	Configure
192.168.168.10	514	

Status: Ready

Syslog Settings

Syslog Facility

- **Syslog Facility** - Allows you to select the facilities and severities of the messages based on the syslog protocol.

Cross Reference: See RCF 3164 - The BSD Syslog Protocol for more information.

- **Override Syslog Settings with ViewPoint Settings** - Check this box to override Syslog settings, if you're using SonicWALL ViewPoint for your reporting solution.

Cross Reference: *For more information on SonicWALL ViewPoint, go to http://www.sonicwall.com.*

  - **Syslog Event Redundancy (seconds)** - This setting prevents repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Event Redundancy Rate** field, they are not written to Syslog as unique events. Instead, the additional events are counted, and then at the end of the period, a message is written to the Syslog that includes the number of times the event occurred. The **Syslog Event Redundancy** default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.
  - **Syslog Format** - You can choose the format of the Syslog to be **Default** or **WebTrends**. If you select **WebTrends**, however, you must have WebTrends software installed on your system.

Alert: *If the SonicWALL security appliance is managed by SonicWALL GMS, the Syslog Server fields cannot be configured by the administrator of the SonicWALL security appliance.*

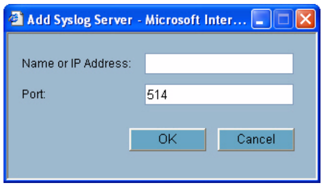
- **Enable Event Rate Limiting** - This control allows you to enable rate limiting of events to prevent the internal or external logging mechanism from being overwhelmed by log events.
- **Enable Data Rate Limiting** - This control allows you to enable rate limiting of data to prevent the internal or external logging mechanism from being overwhelmed by log events.

Syslog Servers

Adding a Syslog Server

To add syslog servers to the SonicWALL security appliance

1. Click **Add**. The **Add Syslog Server** window is displayed.



Name or IP Address:

Port: 514

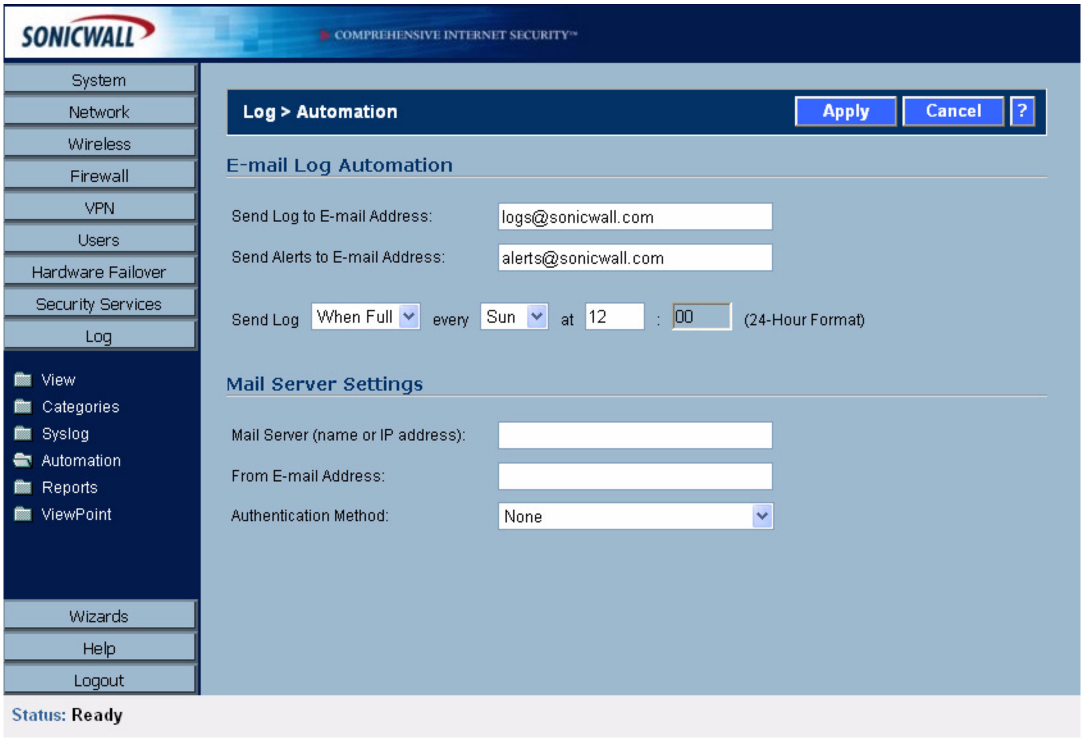
2. Type the Syslog server name or IP address in the **Name or IP Address** field. Messages from the SonicWALL security appliance are then sent to the servers.
3. If your syslog is not using the default port of **514**, type the port number in the **Port Number** field.
4. Click **OK**.
5. Click **Apply** to save all **Syslog Server** settings.

CHAPTER
45

Configuring Log Automation

Log > Automation

The **Log>Automation** page includes settings for configuring the SonicWALL to send log files using e-mail and configuring mail server settings.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
View
Categories
Syslog
Automation
Reports
ViewPoint
Wizards
Help
Logout
Log > Automation
Apply
Cancel
?

E-mail Log Automation

Send Log to E-mail Address: logs@sonicwall.com

Send Alerts to E-mail Address: alerts@sonicwall.com

Send Log When Full every Sun at 12 : 00 (24-Hour Format)

Mail Server Settings

Mail Server (name or IP address):

From E-mail Address:

Authentication Method: None

Status: Ready

E-mail Log Automation

- **Send Log to E-mail address** - enter your e-mail address (username@mydomain.com) in this field to receive the event log via e-mail. Once sent, the log is cleared from the SonicWALL memory. If this field is left blank, the log is not e-mailed.
- **Send Alerts to E-mail address** - enter your e-mail address (username@mydomain.com) in the **Send alerts to** field to be immediately e-mailed when attacks or system errors occur. Type a

standard e-mail address or an e-mail paging service. If this field is left blank, e-mail alert messages are not sent.

- **Send Log** - determines the frequency of sending log files. The options are **When Full**, **Weekly**, or **Daily**. If the **Weekly** or **Daily** option is selected, then select the day of the week the log is sent in the **every** menu and in the **At** field, the time of day in 24-hour format in the

Mail Server Settings

The mail server settings allow you to specify the name or IP address of your mail server, the from e-mail address, and authentication method.

- **Mail Server (name or IP address)** - Enter the IP address or FQDN of the e-mail server used to send your log e-mails in this field.
- **From E-mail Address** - Enter the E-mail address you want to display in the From field of the message.
- **Authentication Method** - You can use the default None item or select **POP Before SMTP**.

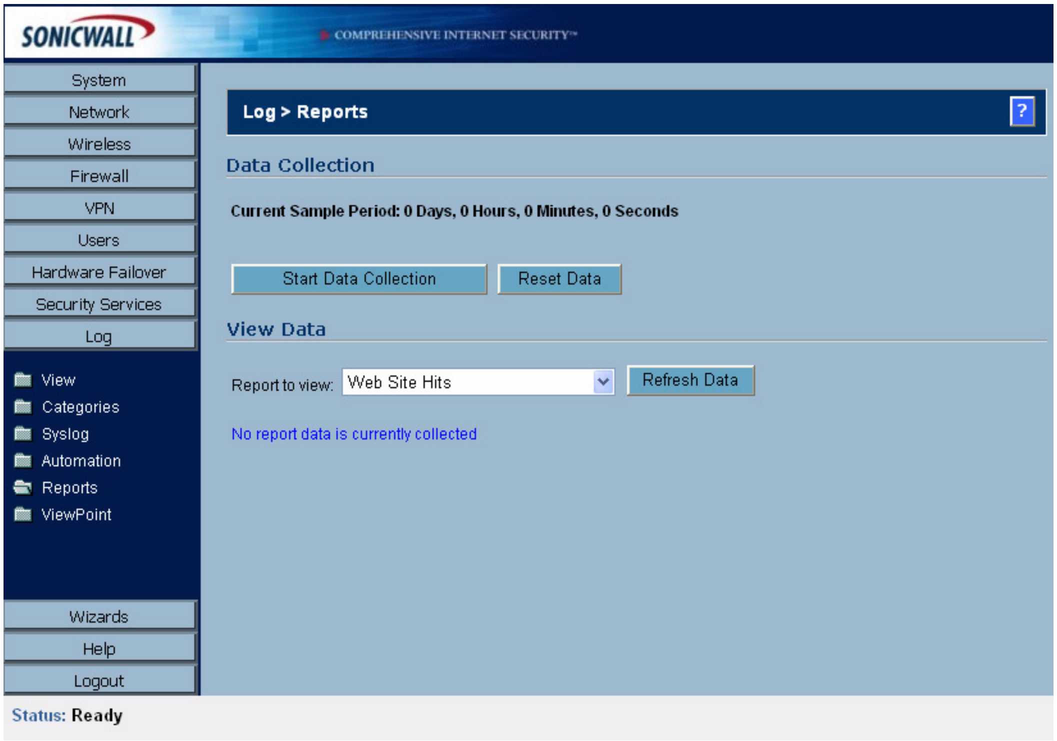
▲ **Alert:** *If the **Mail Server (name or IP address)** is is left blank, log and alert messages are not e-mailed.*

CHAPTER 46

Generating Log Reports

Log > Reports

The SonicWALL security appliance can perform a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. You can generate these reports from the **Log>Reports** page.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
View
Categories
Syslog
Automation
Reports
ViewPoint
Wizards
Help
Logout
Log > Reports
?
Data Collection
Start Data Collection
Reset Data
View Data
Refresh Data

Current Sample Period: 0 Days, 0 Hours, 0 Minutes, 0 Seconds

Report to view: Web Site Hits

No report data is currently collected

Status: Ready

Note: *SonicWALL ViewPoint provides a comprehensive Web-based reporting solution for SonicWALL security appliances. For more information on SonicWALL ViewPoint, go to http://www.sonicwall.com*

Data Collection

The **Reports** window includes the following functions and commands:

- **Start Data Collection**

  Click **Start Data Collection** to begin log analysis. When log analysis is enabled, the button label changes to **Stop Data Collection**.

- **Reset Data**

  Click **Reset Data** to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the SonicWALL security appliance is restarted.

View Data

Select the desired report from the **Report to view** menu. The options are **Web Site Hits**, **Bandwidth Usage by IP Address**, and **Bandwidth Usage by Service**. These reports are explained below. Click **Refresh Data** to update the report. The length of time analyzed by the report is displayed in the **Current Sample Period**.

Web Site Hits

Selecting **Web Site Hits** from the **Report to view** menu displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites.

Bandwidth Usage by IP Address

Selecting **Bandwidth Usage by IP Address** from the **Report to view** menu displays a table showing the IP Address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

Bandwidth Usage by Service

Selecting **Bandwidth Usage by Service** from the **Report to view** menu displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, etc., and the number of megabytes received from the service during the current sample period.

The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.

CHAPTER

47

Activating and Enabling SonicWALL ViewPoint

Log > ViewPoint

SonicWALL ViewPoint is a Web-based graphical reporting tool that provides unprecedented security awareness and control over your network environment through detailed and comprehensive reports of your security and network activities. ViewPoint's broad reporting capabilities allow administrators to easily monitor network access and Internet usage, enhance security, assess risks, understand more about employee Internet use and productivity, and anticipate future bandwidth needs.

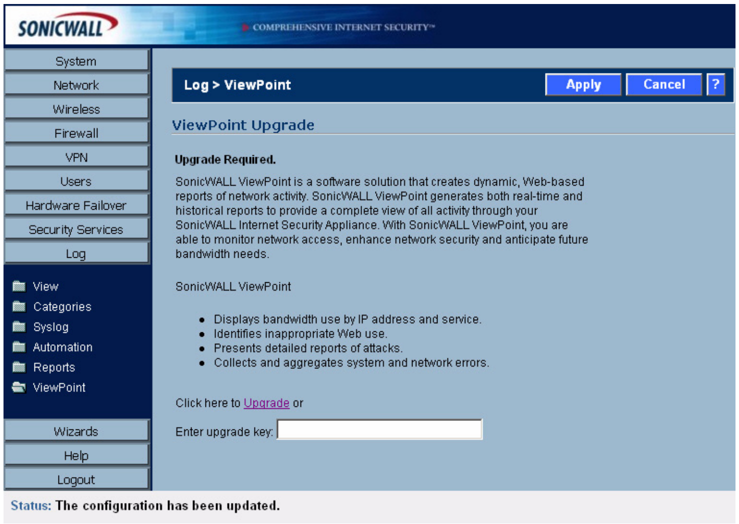
ViewPoint creates dynamic, real-time and historical network summaries, providing a flexible, comprehensive view of network events and activities. Reports are based on syslog data streams received from each SonicWALL appliance through LAN, Wireless LAN, WAN or VPN connections. With ViewPoint, your organization can generate individual or aggregate reports about virtually any aspect of appliance activity, including individual user or group usage patterns, evens on specific appliances or groups of appliances, types and times of attacks, resource consumption and constraints, and more.

➲ **Cross Reference:** *For more information on SonicWALL ViewPoint, go to http://www.sonicwall.com.*

➲ **Cross Reference:** *For complete SonicWALL ViewPoint documentation, go to the SonicWALL documentation Web site at http://www.sonicwall.com/services/documentation.html.*

Activating ViewPoint

The **Log>ViewPoint** page allows you to activate the ViewPoint license directly from the SonicWALL Management Interface using two methods.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
View
Categories
Syslog
Automation
Reports
ViewPoint
Wizards
Help
Logout
Log > ViewPoint
Apply
Cancel
?

ViewPoint Upgrade

Upgrade Required.

SonicWALL ViewPoint is a software solution that creates dynamic, Web-based reports of network activity. SonicWALL ViewPoint generates both real-time and historical reports to provide a complete view of all activity through your SonicWALL Internet Security Appliance. With SonicWALL ViewPoint, you are able to monitor network access, enhance network security and anticipate future bandwidth needs.

SonicWALL ViewPoint

- Displays bandwidth use by IP address and service.
- Identifies inappropriate Web use.
- Presents detailed reports of attacks.
- Collects and aggregates system and network errors.

Click here to Upgrade or

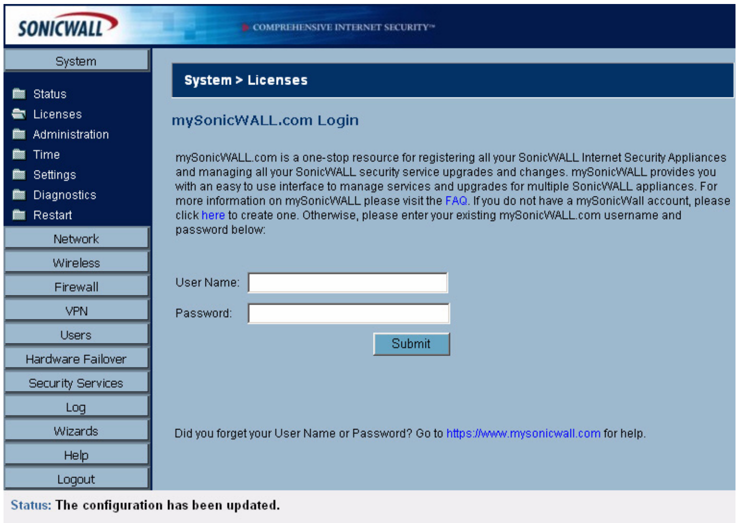
Enter upgrade key:

Status: The configuration has been updated.

If you received a license activation key, enter the activation key in the Enter upgrade key field, and click **Apply**.

Alert: *You must have a mySonicWALL.com account and your SonicWALL security appliance must be registered to activate SonicWALL ViewPoint for your SonicWALl security appliance.*

1 Click the **Upgrade** link in **Click here to Upgrade** on the **Log>ViewPont** page. The **mySonicWALL.com Login** page is displayed.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
Wizards
Help
Logout
System > Licenses
Submit

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall account, please click here to create one. Otherwise, please enter your existing mySonicWALL.com username and password below:

User Name:

Password:

Did you forget your User Name or Password? Go to https://www.mysonicwall.com for help.

Status: The configuration has been updated.

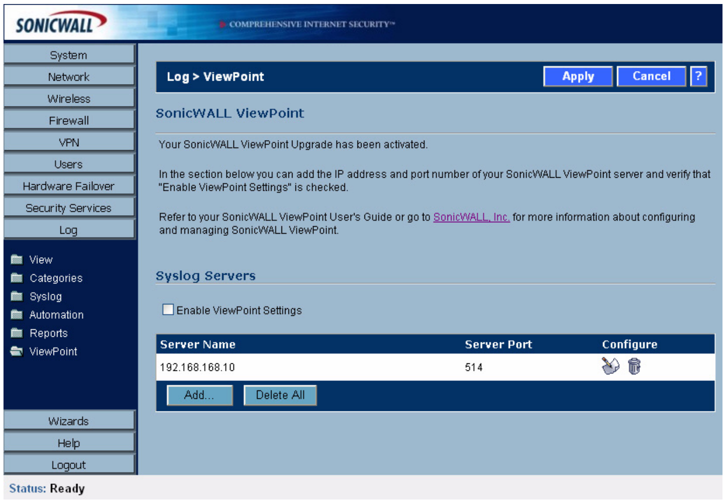
2 Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System>Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System>Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.

3 Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**.

4 If you activated SonicWALL ViewPoint at mySonicWALL.com, the SonicWALL ViewPoint activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services>Summary** page to update your SonicWALL.

Enabling ViewPoint Settings

Once you have installed the SonicWALL ViewPoint software, you can point the SonicWALL security appliance to the server running ViewPoint.


SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Firewall
VPN
Users
Hardware Failover
Security Services
Log
View
Categories
Syslog
Automation
Reports
ViewPoint
Wizards
Help
Logout
Log > ViewPoint
Apply
Cancel
?
Add...
Delete All
Status: Ready

SonicWALL ViewPoint

Your SonicWALL ViewPoint Upgrade has been activated.

In the section below you can add the IP address and port number of your SonicWALL ViewPoint server and verify that "Enable ViewPoint Settings" is checked.

Refer to your SonicWALL ViewPoint User's Guide or go to SonicWALL, Inc. for more information about configuring and managing SonicWALL ViewPoint.

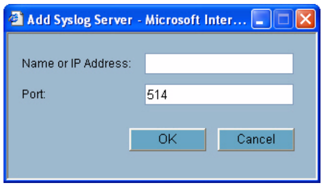
Syslog Servers

☐ Enable ViewPoint Settings

Server Name	Server Port	Configure
192.168.168.10	514	

1 Check the **Enable ViewPoint Settings** checkbox in the **Syslog Servers** section of the **Log>ViewPoint** page.

2 Click the **Add** button. The **Add Syslog Server** window is displayed.


Add Syslog Server - Microsoft Inter...
OK
Cancel

Name or IP Address:

Port: 514

3 Enter the IP address or FQDN of the SonicWALL ViewPoint server in the **Name or IP Address** field.

4 Enter the port number for the SonicWALL ViewPoint server traffic in the **Port** field or use the default port number.

5 Click **Apply**.

Note: *The **Override Syslog Settings with ViewPoint Settings** control on the **Log>Syslog** page is automatically checked when you enable ViewPoint from the **Log>ViewPoint** page. The IP address or FQDN you entered in the **Add Syslog Server** window is also displayed on the **Log>Syslog** page as well as in the **Syslog Servers** table on the **Log>ViewPoint** page.*

Clicking the Edit icon displays the **Add Syslog Server** window for editing the ViewPoint server information. Clicking the Delete (Trashcan) icon, deletes the ViewPoint syslog server entry.

PART

11

Wizards

:

CHAPTER

48

Configuring Internet Connectivity Using the Setup Wizard

Internet Connectivity Using the Setup Wizard

The first time you log into the SonicWALL, the **Setup Wizard** is launched automatically. To launch the **Setup Wizard** at any from the Management Interface, log into the SonicWALL. Click **Wizards** and select **Setup Wizard**.

✓ **Tip:** *You can also configure all your WAN and network settings on the* ***Network>Settings*** *page of the SonicWALL Management Interface*

Configuring a Static IP Address with NAT Enabled

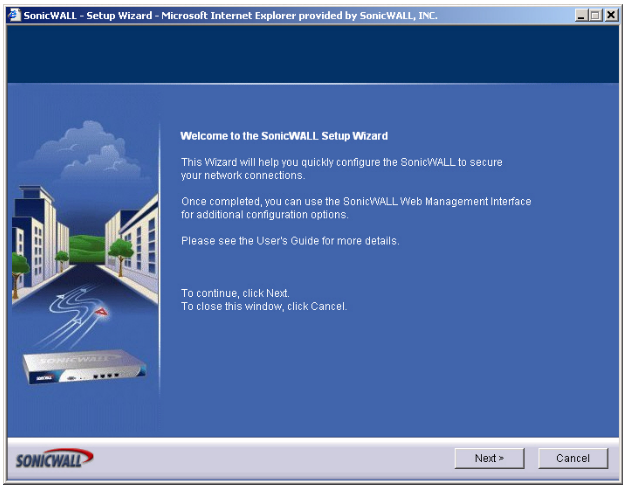
Using NAT to set up your SonicWALL eliminates the need for public IP addresses for all computers on your LAN. It is a way to conserve IP addresses available from the pool of IPv4 addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network. If you do not have enough individual IP addresses for all computers on your network, you can use NAT for your network configuration.

Essentially, NAT translates the IP addresses in one network into those for a different network. As a form of packet filtering for firewalls, it protects a network from outside intrusion from hackers by replacing the internal (LAN) IP address on packets passing through a SonicWALL with a “fake” one from a fixed pool of addresses. The actual IP addresses of computers on the LAN are hidden from outside view.

This section describes configuring the SonicWALL appliance in the NAT mode. If you are assigned a single IP address by your ISP, follow the instructions below.

✓ **Tip:** *Be sure to have your network information including your WAN IP address, subnet mask, and DNS settings ready. This information is obtained from your ISP.*

Setup Wizard


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
Next >
Cancel

Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections.

Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

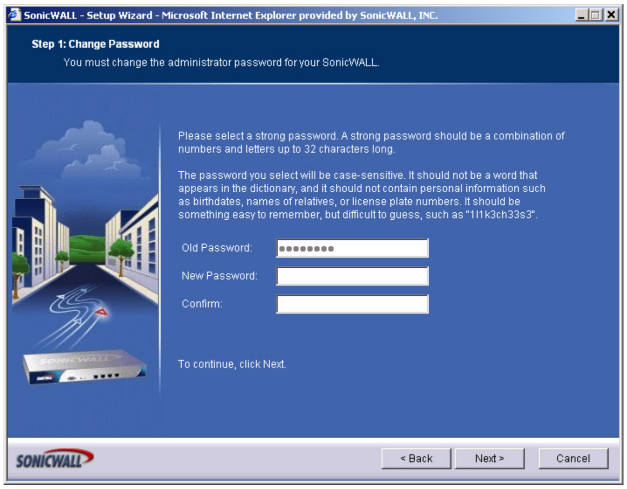
Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

Note: *Your Web browser must be Java-enabled and support HTTP uploads in order to fully manage SonicWALL. Internet Explorer 5.0 and above as well as Netscape Navigator 4.0 and above meet these criteria.*

1 Click the **Setup Wizard** button on the **Network > Settings** page. Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Change Password


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
< Back
Next >
Cancel

Step 1: Change Password

You must change the administrator password for your SonicWALL.

Please select a strong password. A strong password should be a combination of numbers and letters up to 32 characters long.

The password you select will be case-sensitive. It should not be a word that appears in the dictionary, and it should not contain personal information such as birthdates, names of relatives, or license plate numbers. It should be something easy to remember, but difficult to guess, such as "1l1k3ch33s3".

Old Password: ●●●●●●●●

New Password:

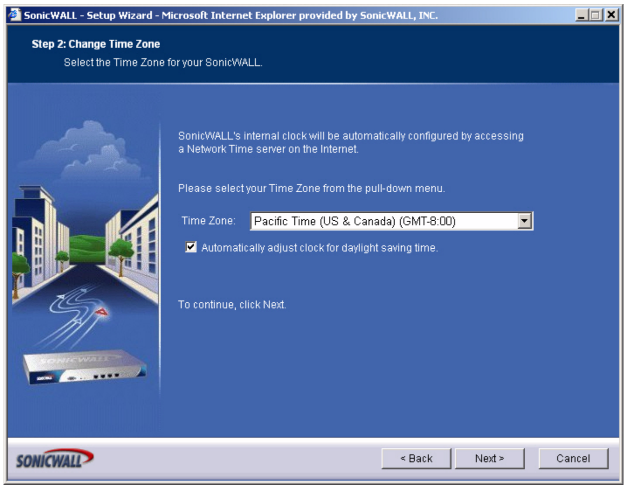
Confirm:

To continue, click Next.

2 To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next.**

Tip: *It is very important to choose a password which cannot be easily guessed by others.*

Step 2: Change Time Zone



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: Change Time Zone

Select the Time Zone for your SonicWALL.

SonicWALL's internal clock will be automatically configured by accessing a Network Time server on the Internet.

Please select your Time Zone from the pull-down menu.

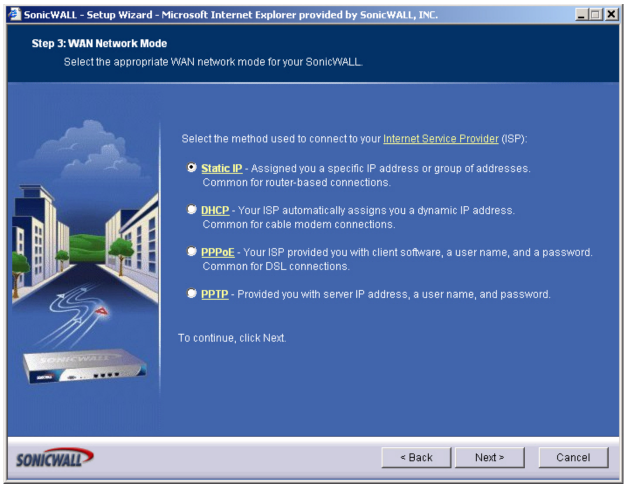
Time Zone: Pacific Time (US & Canada) (GMT-8:00)

☑ Automatically adjust clock for daylight saving time.

To continue, click Next.

3. Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 3: WAN Network Mode



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 3: WAN Network Mode

Select the appropriate WAN network mode for your SonicWALL.

Select the method used to connect to your Internet Service Provider (ISP):

● Static IP - Assigned you a specific IP address or group of addresses. Common for router-based connections.

○ DHCP - Your ISP automatically assigns you a dynamic IP address. Common for cable modem connections.

○ PPPoE - Your ISP provided you with client software, a user name, and a password. Common for DSL connections.

○ PPTP - Provided you with server IP address, a user name, and password.

To continue, click Next.

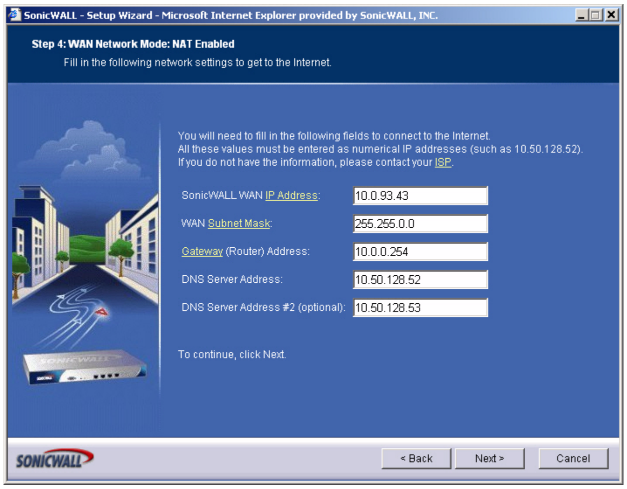
4. Confirm that you have the proper network information necessary to configure the SonicWALL to access the Internet. Click the hyperlinks for definitions of the networking terms.

   You can choose:

- **Static IP**, if your ISP assigns you a specific IP address or group of addresses.
- **DHCP**, if your ISP automatically assigns you a dynamic IP address.
- **PPPoE**, if your ISP provided you with client software, a user name, and a password.
- **PPTP**, if your ISP provided you with a server IP address, a user name, and password.

5. Choose **Static IP** and click **Next**.

Step 4: WAN Network Mode: NAT Enabled


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 4: WAN Network Mode: NAT Enabled

Fill in the following network settings to get to the Internet.

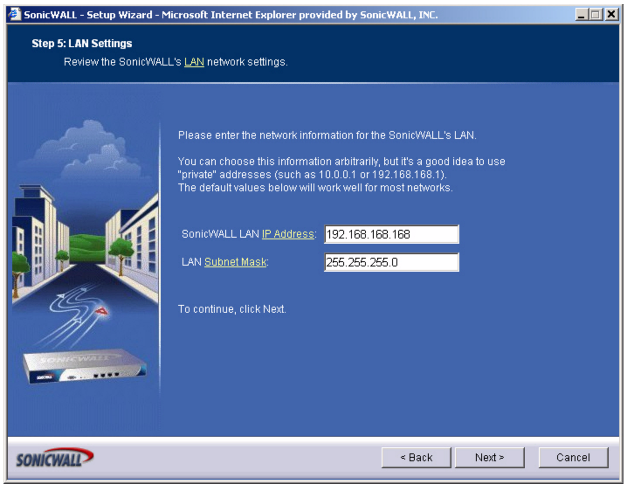
You will need to fill in the following fields to connect to the Internet.
All these values must be entered as numerical IP addresses (such as 10.50.128.52).
If you do not have the information, please contact your ISP.

SonicWALL WAN IP Address: 10.0.93.43
WAN Subnet Mask: 255.255.0.0
Gateway (Router) Address: 10.0.0.254
DNS Server Address: 10.50.128.52
DNS Server Address #2 (optional): 10.50.128.53

To continue, click Next.

6 Enter the public IP address provided by your ISP in the **SonicWALL WAN IP Address**, then fill in the rest of the fields: **WAN/OPT/DMZ Subnet Mask**, **WAN Gateway (Router) Address**, and **DNS Server Addresses**. Click **Next.**

Step 5: LAN Settings


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

Please enter the network information for the SonicWALL's LAN.

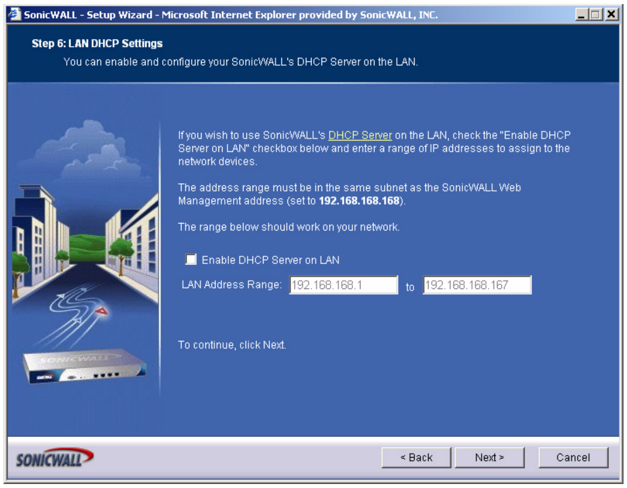
You can choose this information arbitrarily, but it's a good idea to use
"private" addresses (such as 10.0.0.1 or 192.168.168.1).
The default values below will work well for most networks.

SonicWALL LAN IP Address: 192.168.168.168
LAN Subnet Mask: 255.255.255.0

To continue, click Next.

7 The **LAN** page allows the configuration of the **SonicWALL LAN IP Addresses** and the **LAN Subnet Mask.**The **SonicWALL LAN IP Addresses** are the private IP address assigned to the LAN port of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL work for most networks. If you do not use the default settings, enter your preferred private IP address and subnet mask in the fields. Click **Next.**

Step 6: LAN DHCP Settings


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: LAN DHCP Settings

You can enable and configure your SonicWALL's DHCP Server on the LAN.

If you wish to use SonicWALL's DHCP Server on the LAN, check the "Enable DHCP Server on LAN" checkbox below and enter a range of IP addresses to assign to the network devices.

The address range must be in the same subnet as the SonicWALL Web Management address (set to **192.168.168.168**).

The range below should work on your network.

☐ Enable DHCP Server on LAN

LAN Address Range: 192.168.168.1 to 192.168.168.167

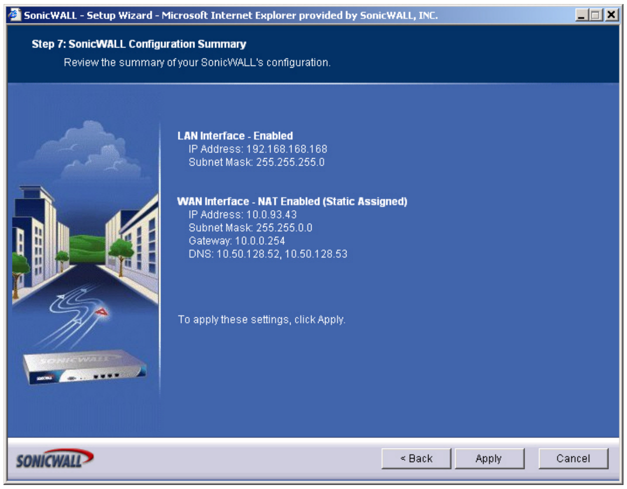
To continue, click Next.

SONICWALL
< Back
Next >
Cancel

8 The **Optional-SonicWALL DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically configures the IP settings of computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next.**

Step 7: SonicWALL Configuration Summary


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 7: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

LAN Interface - Enabled
IP Address: 192.168.168.168
Subnet Mask: 255.255.255.0

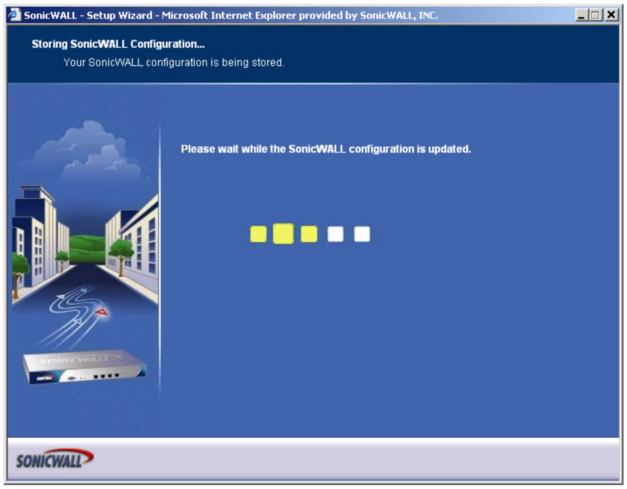
WAN Interface - NAT Enabled (Static Assigned)
IP Address: 10.0.93.43
Subnet Mask: 255.255.0.0
Gateway: 10.0.0.254
DNS: 10.50.128.52, 10.50.128.53

To apply these settings, click Apply.

SONICWALL
< Back
Apply
Cancel

9 The **Configuration Summary** window displays the configuration defined using the Installation Wizard. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next**.

Storing SonicWALL Configuration

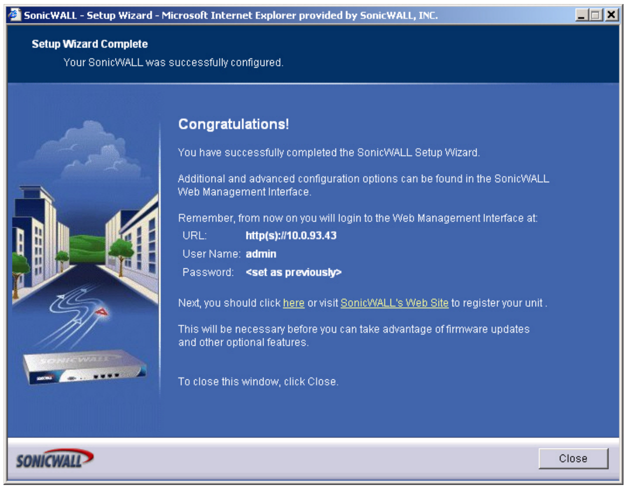

SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL

Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

Setup Wizard Complete


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Close

Setup Wizard Complete

Your SonicWALL was successfully configured.

Congratulations!

You have successfully completed the SonicWALL Setup Wizard.

Additional and advanced configuration options can be found in the SonicWALL Web Management Interface.

Remember, from now on you will login to the Web Management Interface at:
URL: **http(s)://10.0.93.43**
User Name: **admin**
Password: **<set as previously>**

Next, you should click here or visit SonicWALL's Web Site to register your unit .

This will be necessary before you can take advantage of firmware updates and other optional features.

To close this window, click Close.

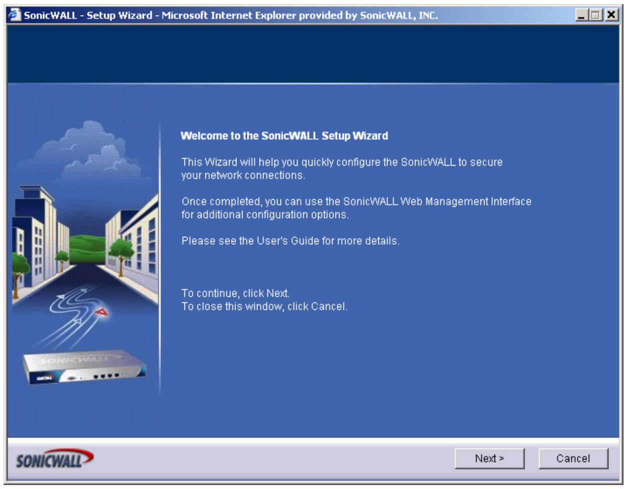
10 The SonicWALL stores the network settings.

11 Click **Restart** to restart the SonicWALL. The SonicWALL takes approximately 90 seconds or longer to restart. During this time, the yellow **Test** LED is lit.

Configuring DHCP Networking Mode

DHCP is a networking mode that allows you to obtain an IP address for a specific length of time from a DHCP server. The length of time is called a lease which is renewed by the DHCP server typically after a few days. When the lease is ready to expire, the client contacts the server to renew the lease. This is a common network configuration for customers with cable or DSL modems. You are not assigned a specific IP address by your ISP.

1 Click the **Setup Wizard** button on the **Network>Settings** page.


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Next >
Cancel

Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections.

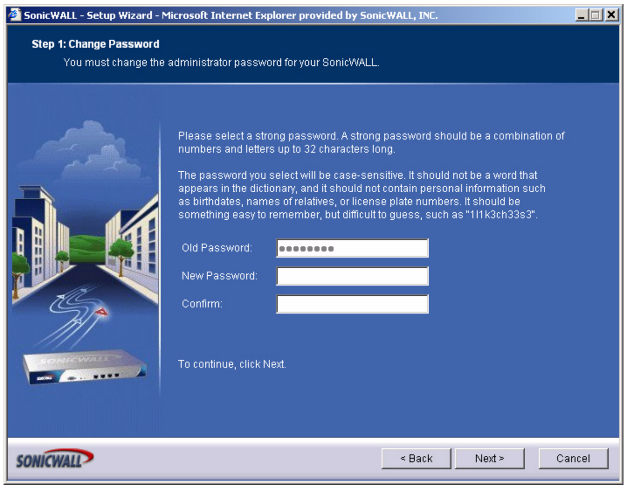
Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

2 Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Change Password


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 1: Change Password
You must change the administrator password for your SonicWALL.

Please select a strong password. A strong password should be a combination of numbers and letters up to 32 characters long.

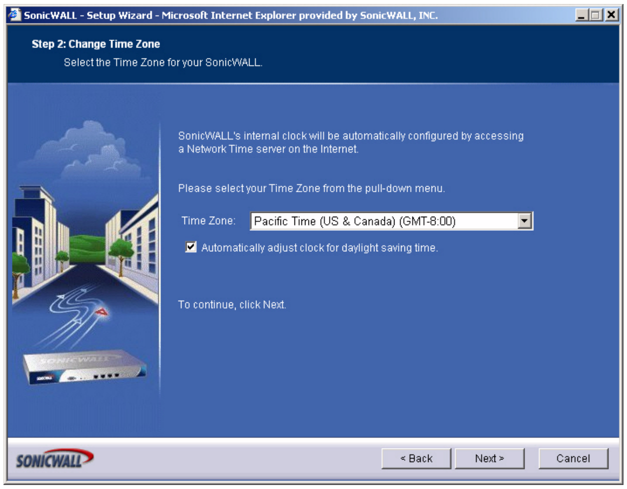
The password you select will be case-sensitive. It should not be a word that appears in the dictionary, and it should not contain personal information such as birthdates, names of relatives, or license plate numbers. It should be something easy to remember, but difficult to guess, such as "1l1k3ch33s3".

Old Password: ••••••••
New Password:
Confirm:

To continue, click Next.

3 To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

Step 2: Change Time Zone


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 2: Change Time Zone
Select the Time Zone for your SonicWALL.

SonicWALL's internal clock will be automatically configured by accessing a Network Time server on the Internet.

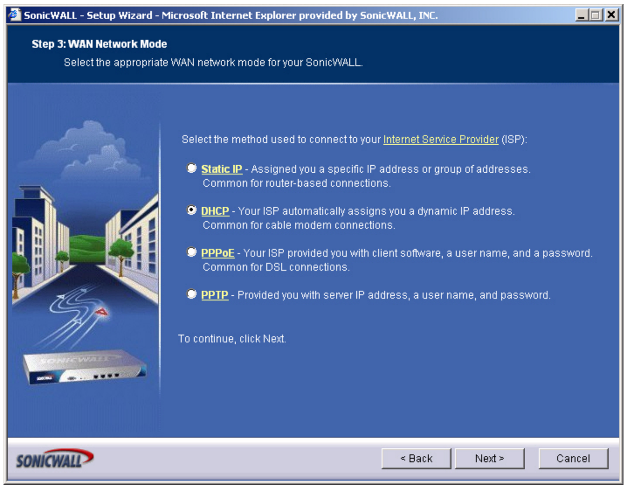
Please select your Time Zone from the pull-down menu.

Time Zone: Pacific Time (US & Canada) (GMT-8:00)
☑ Automatically adjust clock for daylight saving time.

To continue, click Next.

4 Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 3: WAN Network Mode


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 3: WAN Network Mode

Select the appropriate WAN network mode for your SonicWALL.

Select the method used to connect to your Internet Service Provider (ISP):

○ Static IP - Assigned you a specific IP address or group of addresses. Common for router-based connections.

● DHCP - Your ISP automatically assigns you a dynamic IP address. Common for cable modem connections.

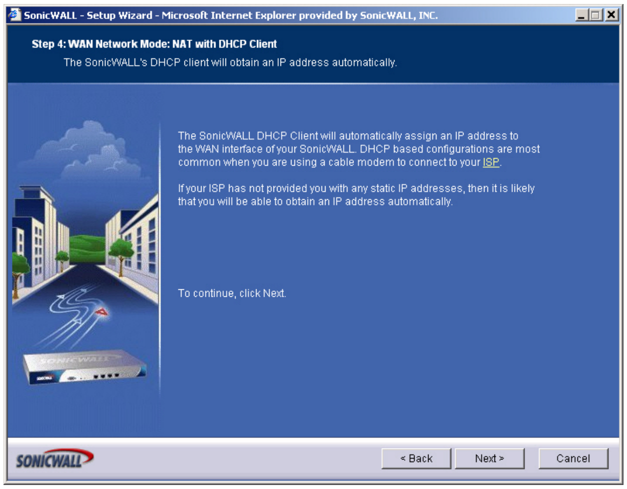
○ PPPoE - Your ISP provided you with client software, a user name, and a password. Common for DSL connections.

○ PPTP - Provided you with server IP address, a user name, and password.

To continue, click Next.

5 Select **DHCP**, the **Obtain an IP address automatically** window is displayed. Click **Next**.

Step 4: WAN Network Mode: NAT with DHCP Client


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 4: WAN Network Mode: NAT with DHCP Client

The SonicWALL's DHCP client will obtain an IP address automatically.

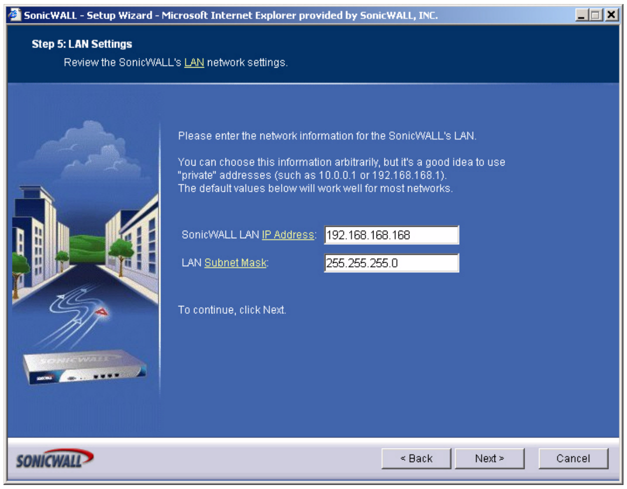
The SonicWALL DHCP Client will automatically assign an IP address to the WAN interface of your SonicWALL. DHCP based configurations are most common when you are using a cable modem to connect to your ISP.

If your ISP has not provided you with any static IP addresses, then it is likely that you will be able to obtain an IP address automatically.

To continue, click Next.

6 The **Obtain an IP address automatically** window states that the ISP dynamically assigns an IP address to the SonicWALL. To confirm this, click **Next.** DHCP-based configurations are most common with cable modem connections.

Step 5: LAN Settings


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

Please enter the network information for the SonicWALL's LAN.

You can choose this information arbitrarily, but it's a good idea to use "private" addresses (such as 10.0.0.1 or 192.168.168.1).
The default values below will work well for most networks.

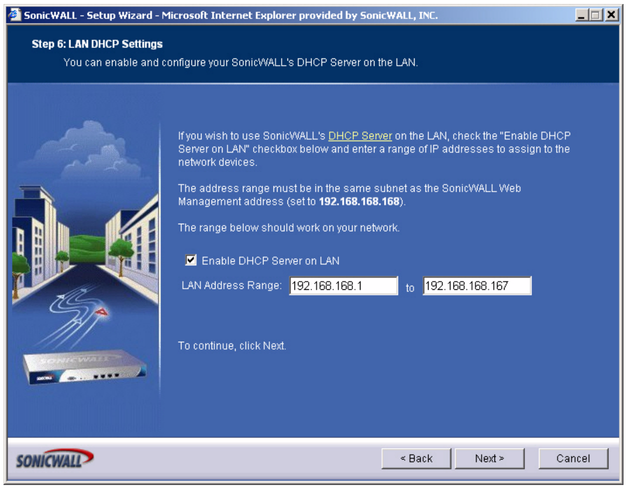
SonicWALL LAN IP Address: 192.168.168.168

LAN Subnet Mask: 255.255.255.0

To continue, click Next.

7. The **Fill in information about your LAN** page allows the configuration of SonicWALL LAN IP Addresses and Subnet Masks. SonicWALL LAN IP Addresses are the private IP addresses assigned to the LAN of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the networks. The default values provided by the SonicWALL are useful for most networks. Click **Next**.

Step 6: DHCP Settings


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 6: LAN DHCP Settings

You can enable and configure your SonicWALL's DHCP Server on the LAN.

If you wish to use SonicWALL's DHCP Server on the LAN, check the "Enable DHCP Server on LAN" checkbox below and enter a range of IP addresses to assign to the network devices.

The address range must be in the same subnet as the SonicWALL Web Management address (set to **192.168.168.168**).

The range below should work on your network.

☑ Enable DHCP Server on LAN

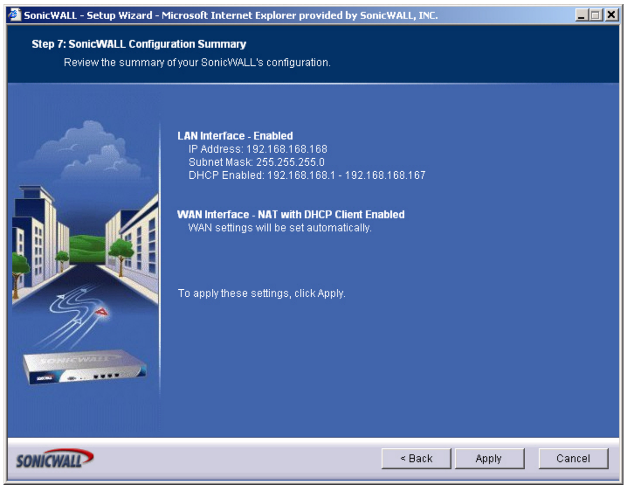
LAN Address Range: 192.168.168.1 to 192.168.168.167

To continue, click Next.

8. The **Optional-SonicWALL DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses assigned to computers on the LAN.

   If **Enable DHCP Server** is not selected, the DHCP Server is disabled. Click **Next** to continue.

Configuration Summary


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 7: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

LAN Interface - Enabled
IP Address: 192.168.168.168
Subnet Mask: 255.255.255.0
DHCP Enabled: 192.168.168.1 - 192.168.168.167

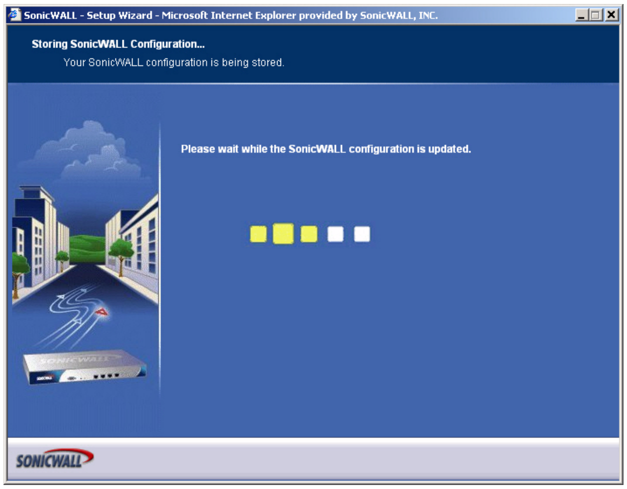
WAN Interface - NAT with DHCP Client Enabled
WAN settings will be set automatically.

To apply these settings, click Apply.

< Back
Apply
Cancel

9 The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Apply.**

Storing SonicWALL Configuration



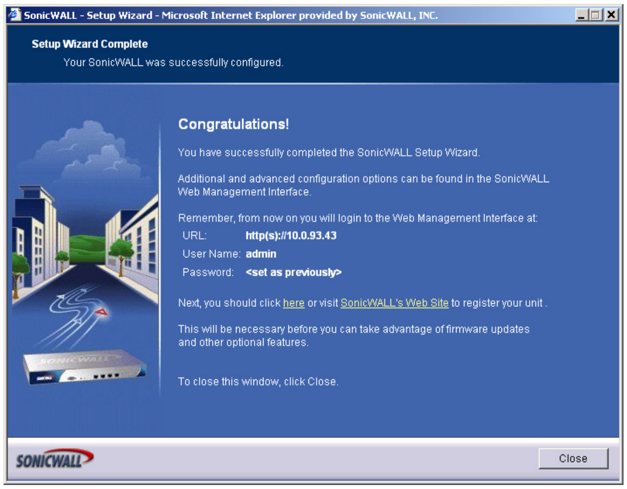
SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL

Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

Setup Wizard Complete



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Close

Setup Wizard Complete

Your SonicWALL was successfully configured.

Congratulations!

You have successfully completed the SonicWALL Setup Wizard.

Additional and advanced configuration options can be found in the SonicWALL Web Management Interface.

Remember, from now on you will login to the Web Management Interface at:

URL: **http(s)://10.0.93.43**
User Name: **admin**
Password: **<set as previously>**

Next, you should click here or visit SonicWALL's Web Site to register your unit .

This will be necessary before you can take advantage of firmware updates and other optional features.

To close this window, click Close.

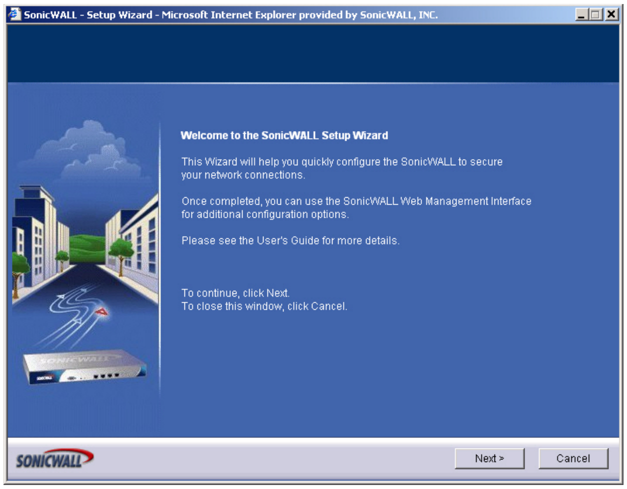
10 Click **Restart** to restart the SonicWALL. The SonicWALL takes 90 seconds to restart. During this time, the yellow **Test** LED is lit.

✓ **Tip:** *The new SonicWALL LAN IP address, displayed in the* ***URL*** *field of the* ***Congratulations*** *window, is used to log in and manage the SonicWALL.*

Configuring NAT Enabled with PPPoE

NAT with PPPoE Client is a network protocol that uses Point to Point Protocol over Ethernet to connect with a remote site using various Remote Access Service products. This protocol is typically found when using a DSL modem with an ISP requiring a user name and password to log into the remote server. The ISP may then allow you to obtain an IP address automatically or give you a specific IP address.

1 Click the **Setup Wizard** button on the **Network>Settings** page.


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
Next >
Cancel
SONICWALL

Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections.

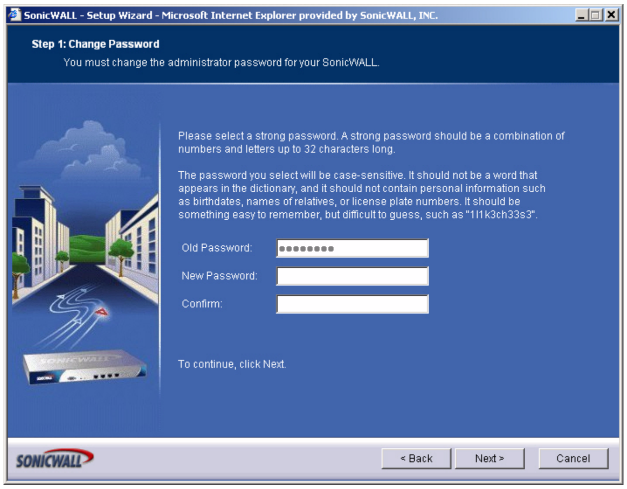
Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

2 Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Change Password


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
< Back
Next >
Cancel
SONICWALL

Step 1: Change Password

You must change the administrator password for your SonicWALL.

Please select a strong password. A strong password should be a combination of numbers and letters up to 32 characters long.

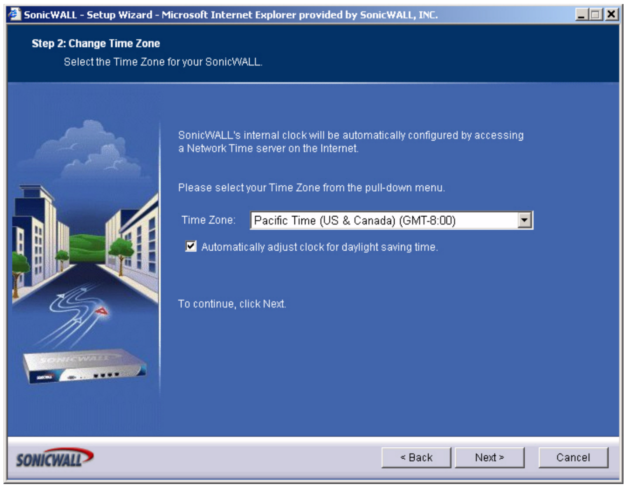
The password you select will be case-sensitive. It should not be a word that appears in the dictionary, and it should not contain personal information such as birthdates, names of relatives, or license plate numbers. It should be something easy to remember, but difficult to guess, such as "1l1k3ch33s3".

Old Password: ••••••••
New Password:
Confirm:

To continue, click Next.

3 To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next.**

Step 2: Change Time Zone


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 2: Change Time Zone

Select the Time Zone for your SonicWALL.

SonicWALL's internal clock will be automatically configured by accessing a Network Time server on the Internet.

Please select your Time Zone from the pull-down menu.

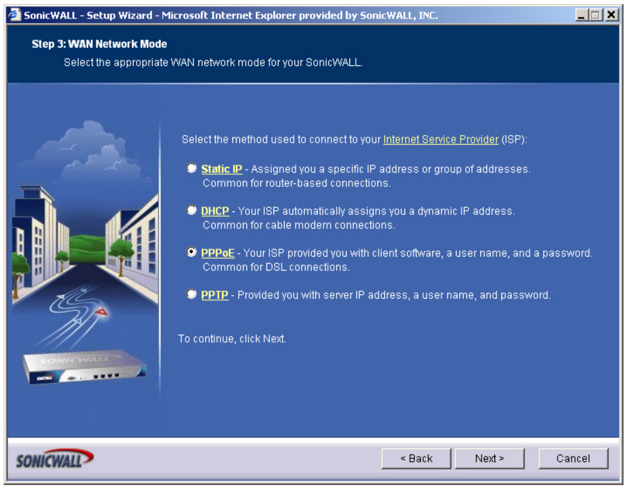
Time Zone: Pacific Time (US & Canada) (GMT-8:00)

☑ Automatically adjust clock for daylight saving time.

To continue, click Next.

4 Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 3: WAN Network Mode


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 3: WAN Network Mode

Select the appropriate WAN network mode for your SonicWALL.

Select the method used to connect to your Internet Service Provider (ISP):

○ Static IP - Assigned you a specific IP address or group of addresses. Common for router-based connections.

○ DHCP - Your ISP automatically assigns you a dynamic IP address. Common for cable modem connections.

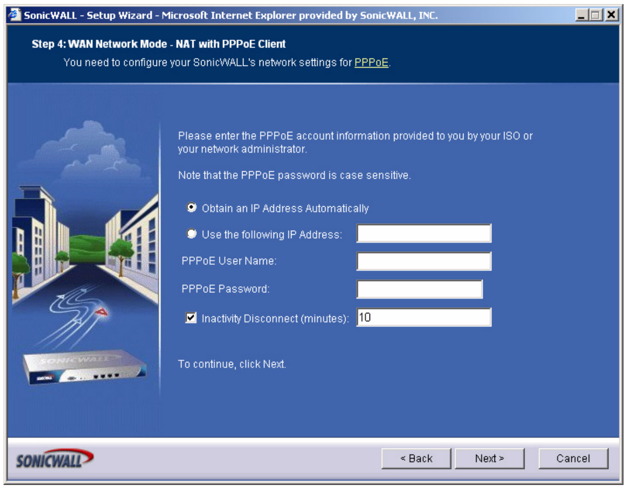
● PPPoE - Your ISP provided you with client software, a user name, and a password. Common for DSL connections.

○ PPTP - Provided you with server IP address, a user name, and password.

To continue, click Next.

5 The SonicWALL automatically detects the presence of a PPPoE server on the WAN. If not, then select **PPPoE: Your ISP provided you with desktop software, a user name and password**. Click **Next**.

Step 4: WAN Network Mode: NAT with PPPoE Client


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode - NAT with PPPoE Client

You need to configure your SonicWALL's network settings for PPPoE.

Please enter the PPPoE account information provided to you by your ISO or your network administrator.

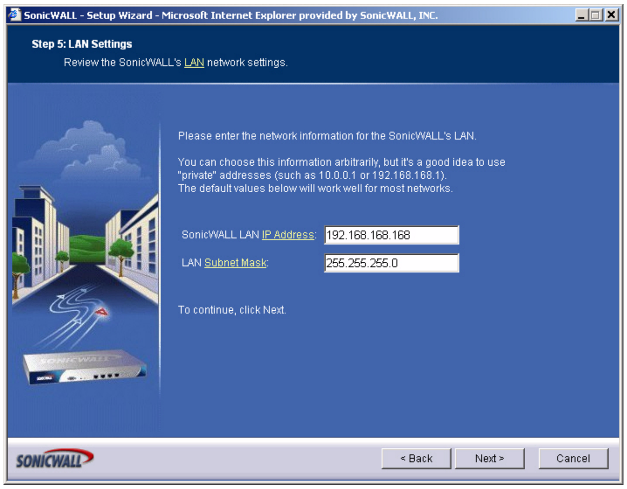
Note that the PPPoE password is case sensitive.

● Obtain an IP Address Automatically
○ Use the following IP Address:
PPPoE User Name:
PPPoE Password:
☑ Inactivity Disconnect (minutes): 10

To continue, click Next.

6 Select whether to use a dynamic or static IP address, and enter the user name and password provided by your ISP into the **User Name** and **Password** fields. Click **Next**.

Step 5: LAN Settings


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

Please enter the network information for the SonicWALL's LAN.

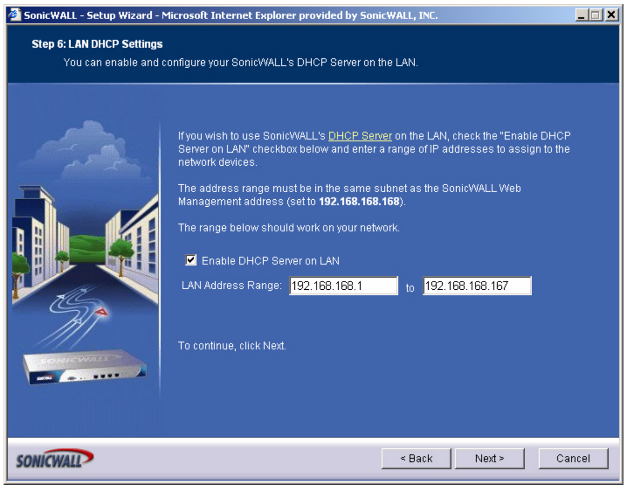
You can choose this information arbitrarily, but it's a good idea to use "private" addresses (such as 10.0.0.1 or 192.168.168.1).
The default values below will work well for most networks.

SonicWALL LAN IP Address: 192.168.168.168
LAN Subnet Mask: 255.255.255.0

To continue, click Next.

7 The **LAN Settings** page allows the configuration of SonicWALL LAN IP Addresses and LAN Subnet Mask.The SonicWALL LAN IP Address is the private IP address assigned to the LAN port of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL are useful for most networks. If you do not use the default settings, enter your preferred IP addresses in the fields. Click **Next**.

Step 6: DHCP Server


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: LAN DHCP Settings

You can enable and configure your SonicWALL's DHCP Server on the LAN.

If you wish to use SonicWALL's DHCP Server on the LAN, check the "Enable DHCP Server on LAN" checkbox below and enter a range of IP addresses to assign to the network devices.

The address range must be in the same subnet as the SonicWALL Web Management address (set to **192.168.168.168**).

The range below should work on your network.

☑ Enable DHCP Server on LAN

LAN Address Range: 192.168.168.1 to 192.168.168.167

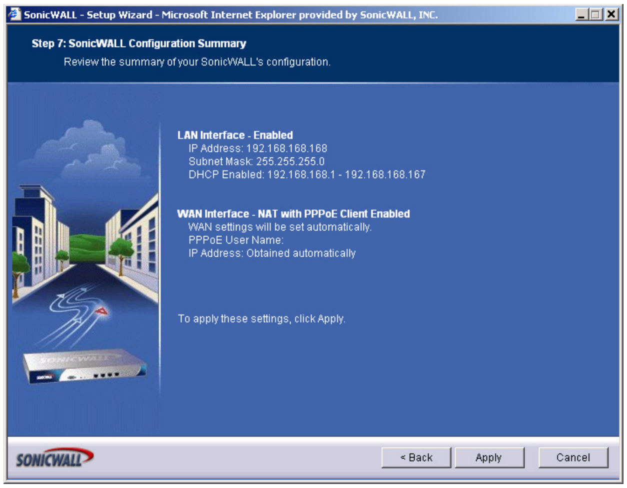
To continue, click Next.

SONICWALL
< Back
Next >
Cancel

8 The **Optional-SonicWALL DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next.**

Step 7: SonicWALL Configuration Summary


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 7: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

LAN Interface - Enabled
IP Address: 192.168.168.168
Subnet Mask: 255.255.255.0
DHCP Enabled: 192.168.168.1 - 192.168.168.167

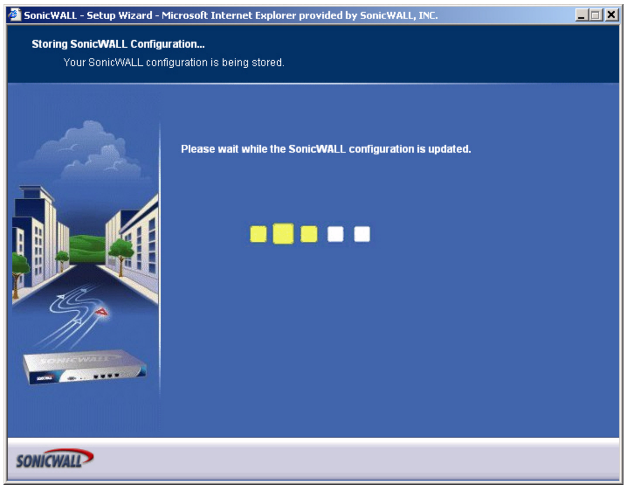
WAN Interface - NAT with PPPoE Client Enabled
WAN settings will be set automatically.
PPPoE User Name:
IP Address: Obtained automatically

To apply these settings, click Apply.

SONICWALL
< Back
Apply
Cancel

9 The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. To modify any of the settings, click **Back** to return to the **WAN Settings** window. If the configuration is correct, click **Next** to proceed to the **Congratulations** window.

Storing SonicWALL Configuration


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL

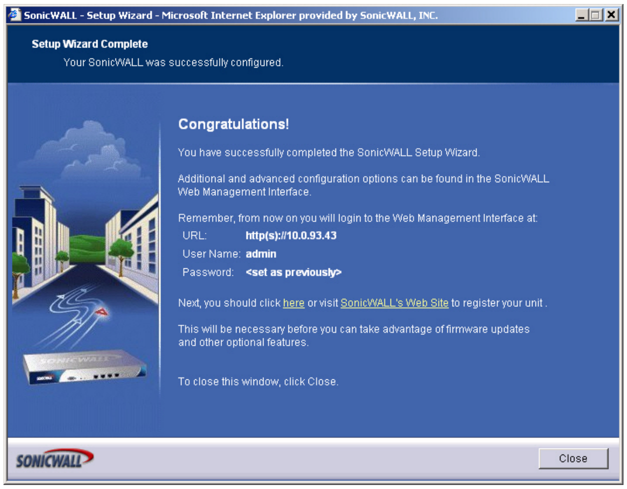
Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

✓ **Tip:** *The new SonicWALL LAN IP address, displayed in the* ***URL*** *field of the* ***Congratulations*** *window, is used to log in and manage the SonicWALL.*

Setup Wizard Complete


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Close

Setup Wizard Complete

Your SonicWALL was successfully configured.

Congratulations!

You have successfully completed the SonicWALL Setup Wizard.

Additional and advanced configuration options can be found in the SonicWALL Web Management Interface.

Remember, from now on you will login to the Web Management Interface at:

URL: **http(s)://10.0.93.43**
User Name: **admin**
Password: **<set as previously>**

Next, you should click here or visit SonicWALL's Web Site to register your unit .

This will be necessary before you can take advantage of firmware updates and other optional features.

To close this window, click Close.

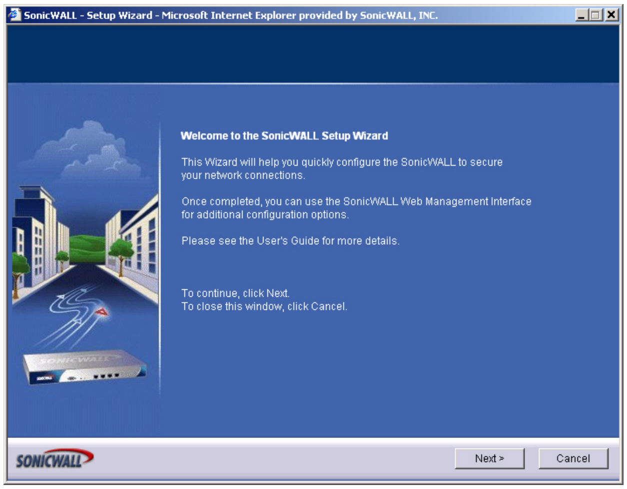
10 Click **Restart** to restart the SonicWALL.

11 The SonicWALL takes approximately 90 seconds or longer to restart. During this time, the yellow **Test** LED is lit.

Configuring PPTP Network Mode

NAT with PPTP Client mode uses Point to Point Tunneling Protocol (PPTP) to connect to a remote server. It supports older Microsoft implementations requiring tunneling connectivity.

1. Click the **Setup Wizard** button on the **Network>Settings** page.


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
Next >
Cancel
SONICWALL

Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections.

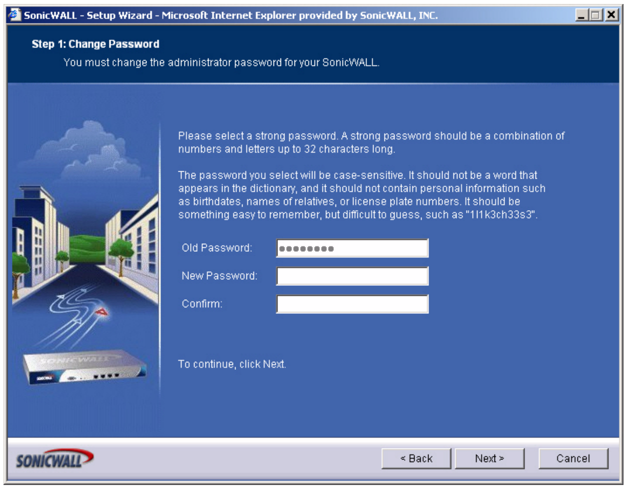
Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

2. Read the instructions on the **Welcome** window and click **Next** to continue.

Step 1: Change Password


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
< Back
Next >
Cancel
SONICWALL

Step 1: Change Password
You must change the administrator password for your SonicWALL.

Please select a strong password. A strong password should be a combination of numbers and letters up to 32 characters long.

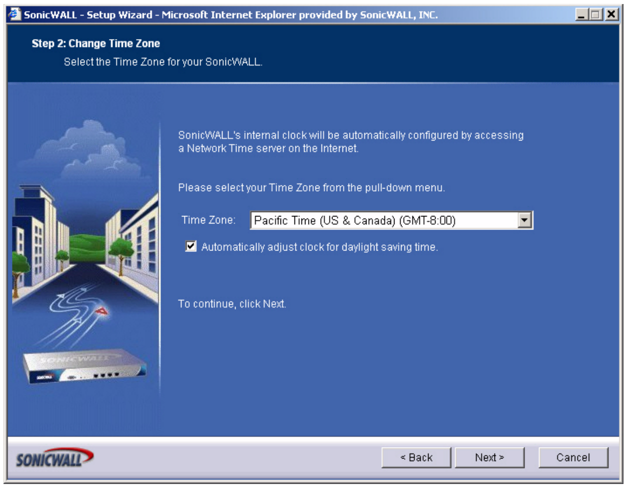
The password you select will be case-sensitive. It should not be a word that appears in the dictionary, and it should not contain personal information such as birthdates, names of relatives, or license plate numbers. It should be something easy to remember, but difficult to guess, such as "1l1k3ch33s3".

Old Password: ●●●●●●●●●
New Password:
Confirm:

To continue, click Next.

3. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

Step 2: Change Time Zone


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
< Back
Next >
Cancel

Step 2: Change Time Zone

Select the Time Zone for your SonicWALL.

SonicWALL's internal clock will be automatically configured by accessing a Network Time server on the Internet.

Please select your Time Zone from the pull-down menu.

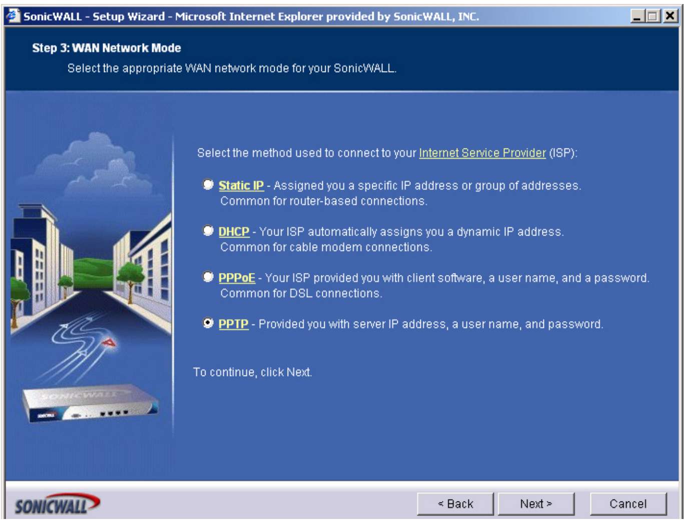
Time Zone: Pacific Time (US & Canada) (GMT-8:00)

☑ Automatically adjust clock for daylight saving time.

To continue, click Next.

4 Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

Step 3: WAN Network Mode


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
< Back
Next >
Cancel

Step 3: WAN Network Mode

Select the appropriate WAN network mode for your SonicWALL.

Select the method used to connect to your Internet Service Provider (ISP):

○ Static IP - Assigned you a specific IP address or group of addresses. Common for router-based connections.

○ DHCP - Your ISP automatically assigns you a dynamic IP address. Common for cable modem connections.

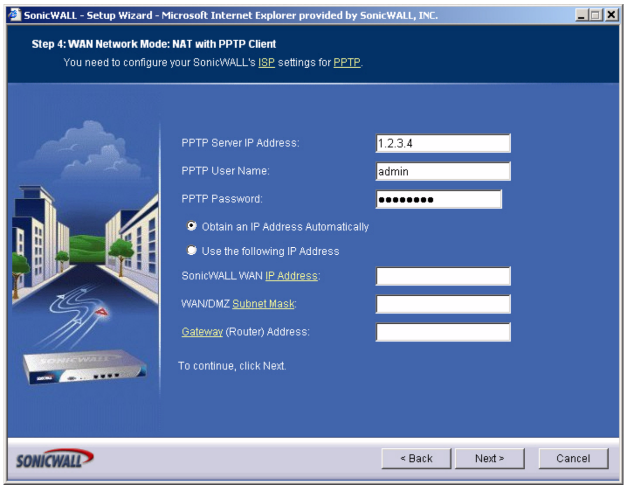
○ PPPoE - Your ISP provided you with client software, a user name, and a password. Common for DSL connections.

● PPTP - Provided you with server IP address, a user name, and password.

To continue, click Next.

5 Select **PPTP: Provided you with a server IP address, a user name and password.** Click **Next**.

Step 4: WAN Network Mode: NAT with PPTP Client


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode: NAT with PPTP Client

You need to configure your SonicWALL's ISP settings for PPTP.

PPTP Server IP Address: 1.2.3.4

PPTP User Name: admin

PPTP Password: ••••••••

● Obtain an IP Address Automatically

○ Use the following IP Address

SonicWALL WAN IP Address:

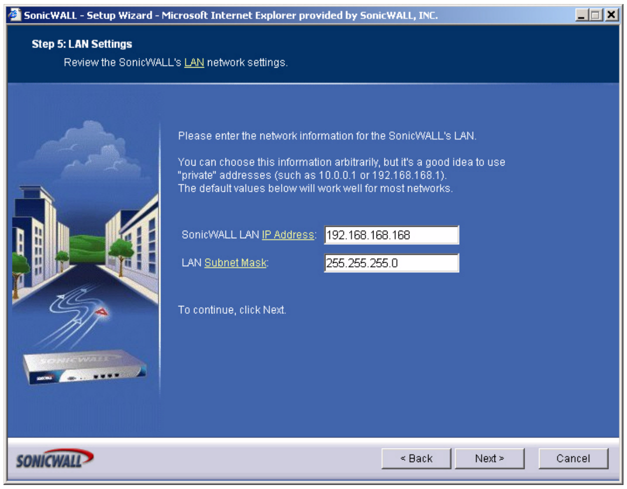
WAN/DMZ Subnet Mask:

Gateway (Router) Address:

To continue, click Next.

6 Enter the user name and password provided by your ISP into the **User Name** and **Password** fields. Click **Next**.

Step 5: LAN Settings


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

Please enter the network information for the SonicWALL's LAN.

You can choose this information arbitrarily, but it's a good idea to use "private" addresses (such as 10.0.0.1 or 192.168.168.1). The default values below will work well for most networks.

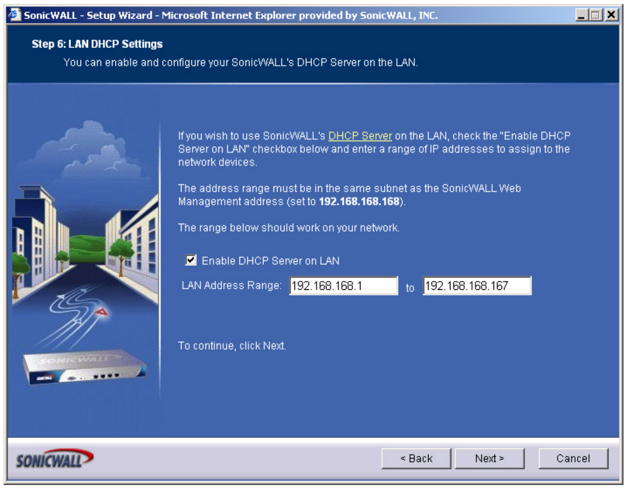
SonicWALL LAN IP Address: 192.168.168.168

LAN Subnet Mask: 255.255.255.0

To continue, click Next.

7 The **LAN Settings** page allows the configuration of SonicWALL LAN IP Addresses and LAN Subnet Mask.The SonicWALL LAN IP Address is the private IP address assigned to the LAN port of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL are useful for most networks. If you do not use the default settings, enter your preferred IP addresses in the fields. Click **Next**.

Step 6: DHCP Server


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
< Back
Next >
Cancel

Step 6: LAN DHCP Settings

You can enable and configure your SonicWALL's DHCP Server on the LAN.

If you wish to use SonicWALL's DHCP Server on the LAN, check the "Enable DHCP Server on LAN" checkbox below and enter a range of IP addresses to assign to the network devices.

The address range must be in the same subnet as the SonicWALL Web Management address (set to **192.168.168.168**).

The range below should work on your network.

☑ Enable DHCP Server on LAN

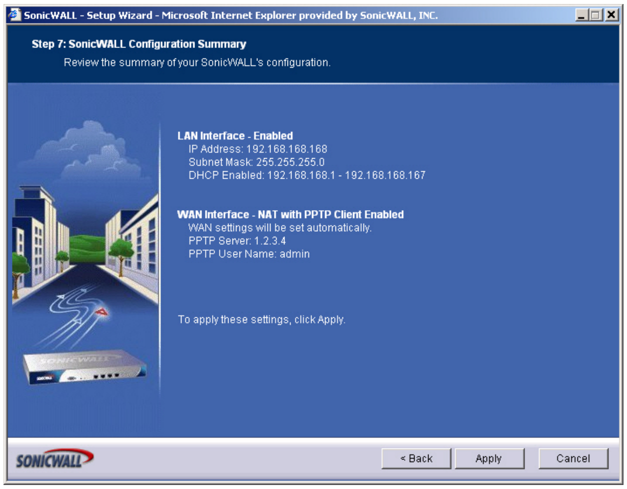
LAN Address Range: 192.168.168.1 to 192.168.168.167

To continue, click Next.

8 The **Optional-SonicWALL DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

If **Enable DHCP Server** is not selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

Step 7: SonicWALL Configuration Summary


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
< Back
Apply
Cancel

Step 7: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

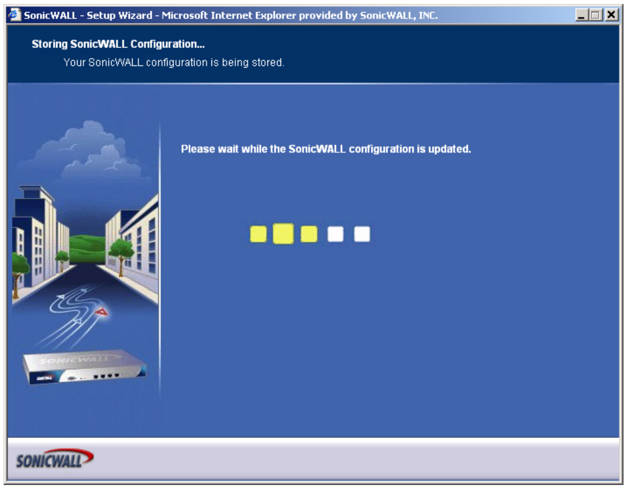
LAN Interface - Enabled
IP Address: 192.168.168.168
Subnet Mask: 255.255.255.0
DHCP Enabled: 192.168.168.1 - 192.168.168.167

WAN Interface - NAT with PPTP Client Enabled
WAN settings will be set automatically.
PPTP Server: 1.2.3.4
PPTP User Name: admin

To apply these settings, click Apply.

9 The **Configuration Summary** window displays the configuration defined using the **Installation Wizard**. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next** to proceed to the **Storing SonicWALL Configuration** window.

Storing SonicWALL Configuration


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL

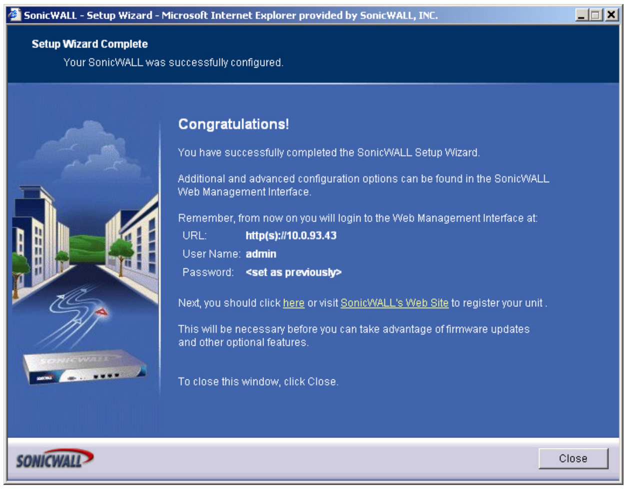
Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

✓ **Tip:** *The new SonicWALL LAN IP address, displayed in the* ***URL*** *field of the* ***Congratulations*** *window, is used to log in and manage the SonicWALL.*

Setup Wizard Complete


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Close

Setup Wizard Complete

Your SonicWALL was successfully configured.

Congratulations!

You have successfully completed the SonicWALL Setup Wizard.

Additional and advanced configuration options can be found in the SonicWALL Web Management Interface.

Remember, from now on you will login to the Web Management Interface at:
URL: **http(s)://10.0.93.43**
User Name: **admin**
Password: **<set as previously>**

Next, you should click here or visit SonicWALL's Web Site to register your unit .

This will be necessary before you can take advantage of firmware updates and other optional features.

To close this window, click Close.

10 Click **Restart** to restart the SonicWALL. The SonicWALL takes approximately 90 seconds or longer to restart. During this time, the yellow **Test** LED is lit.

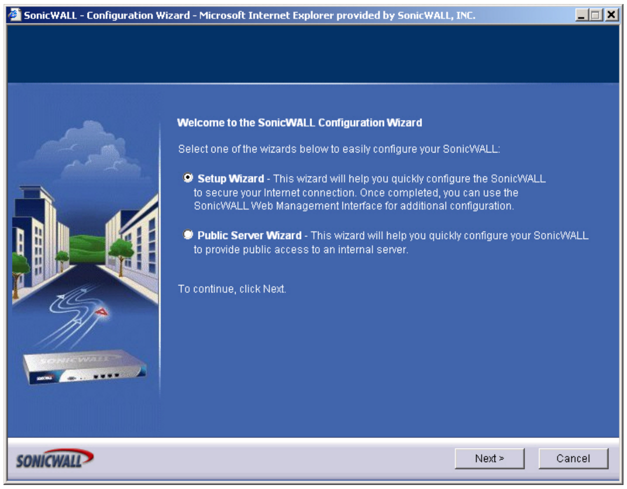
CHAPTER

49

Configuring a Public Server with the Wizard

Create a Server with the Public Server Wizard

1 Start wizard: In the navigator, click **Wizards**.



SonicWALL - Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Welcome to the SonicWALL Configuration Wizard

Select one of the wizards below to easily configure your SonicWALL:

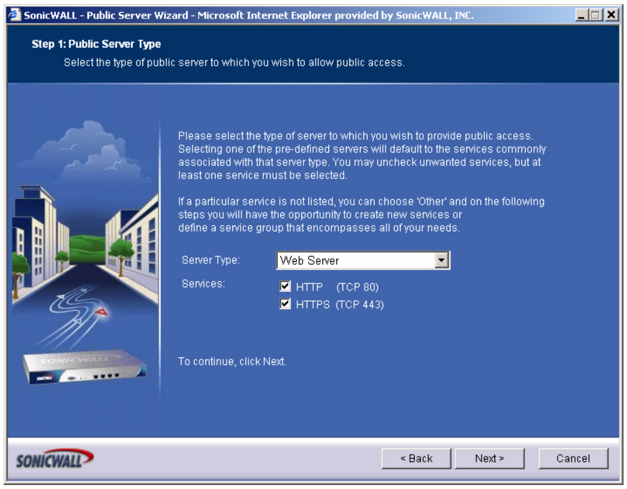
● **Setup Wizard** - This wizard will help you quickly configure the SonicWALL to secure your Internet connection. Once completed, you can use the SonicWALL Web Management Interface for additional configuration.

○ **Public Server Wizard** - This wizard will help you quickly configure your SonicWALL to provide public access to an internal server.

To continue, click Next.

Next >
Cancel

2 Select **Public Server Wizard** and click **Next**.



SonicWALL - Public Server Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: Public Server Type

Select the type of public server to which you wish to allow public access.

Please select the type of server to which you wish to provide public access. Selecting one of the pre-defined servers will default to the services commonly associated with that server type. You may uncheck unwanted services, but at least one service must be selected.

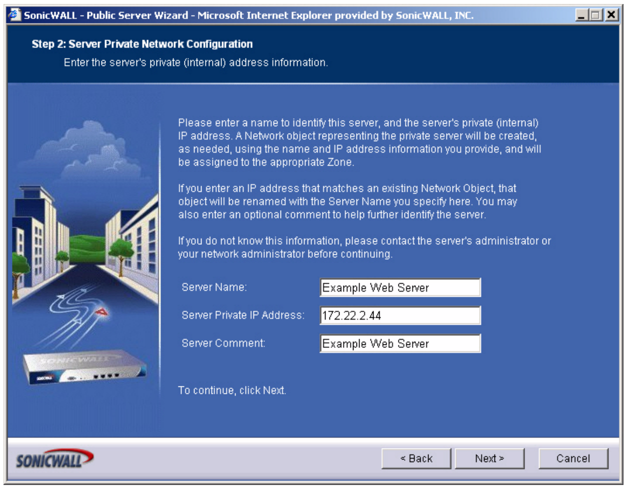
If a particular service is not listed, you can choose 'Other' and on the following steps you will have the opportunity to create new services or define a service group that encompasses all of your needs.

Server Type: Web Server

Services:
☑ HTTP (TCP 80)
☑ HTTPS (TCP 443)

To continue, click Next.

3 Select the type of server from the **Server Type** list. Depending on the type you select, the available services change. Check the box for the services you are enabling on this server. Click **Next**



SonicWALL - Public Server Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: Server Private Network Configuration

Enter the server's private (internal) address information.

Please enter a name to identify this server, and the server's private (internal) IP address. A Network object representing the private server will be created, as needed, using the name and IP address information you provide, and will be assigned to the appropriate Zone.

If you enter an IP address that matches an existing Network Object, that object will be renamed with the Server Name you specify here. You may also enter an optional comment to help further identify the server.

If you do not know this information, please contact the server's administrator or your network administrator before continuing.

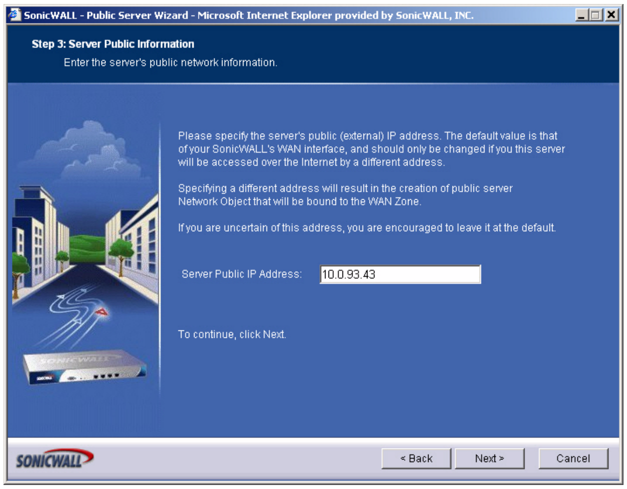
Server Name: Example Web Server
Server Private IP Address: 172.22.2.44
Server Comment: Example Web Server

To continue, click Next.

4 Enter the name of the server.

5 Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to zone where you want to put this server. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs.

6 Click **Next**.


SonicWALL - Public Server Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 3: Server Public Information

Enter the server's public network information.

Please specify the server's public (external) IP address. The default value is that of your SonicWALL's WAN interface, and should only be changed if you this server will be accessed over the Internet by a different address.

Specifying a different address will result in the creation of public server Network Object that will be bound to the WAN Zone.

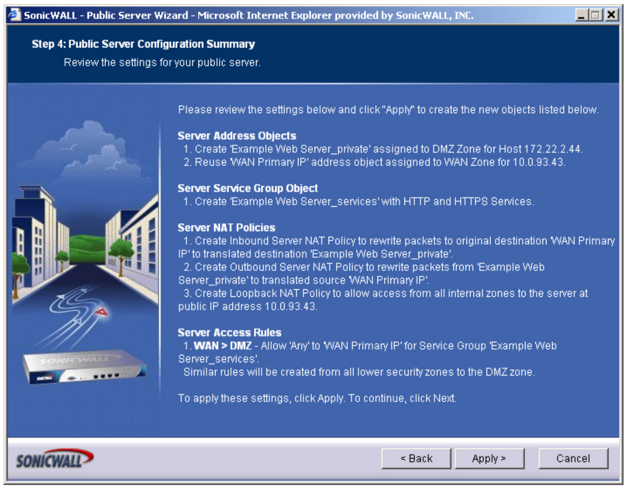
If you are uncertain of this address, you are encouraged to leave it at the default.

Server Public IP Address: 10.0.93.43

To continue, click Next.

7 Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

8 Click **Next**.


SonicWALL - Public Server Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Apply >
Cancel

Step 4: Public Server Configuration Summary

Review the settings for your public server.

Please review the settings below and click "Apply" to create the new objects listed below.

Server Address Objects
1. Create 'Example Web Server_private' assigned to DMZ Zone for Host 172.22.2.44.
2. Reuse 'WAN Primary IP' address object assigned to WAN Zone for 10.0.93.43.

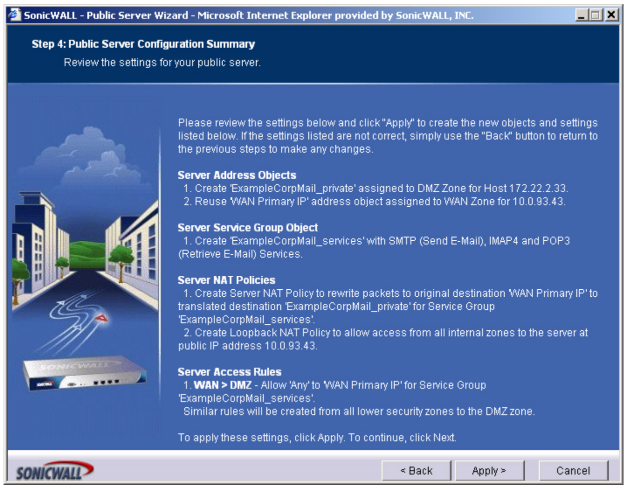
Server Service Group Object
1. Create 'Example Web Server_services' with HTTP and HTTPS Services.

Server NAT Policies
1. Create Inbound Server NAT Policy to rewrite packets to original destination 'WAN Primary IP' to translated destination 'Example Web Server_private'.
2. Create Outbound Server NAT Policy to rewrite packets from 'Example Web Server_private' to translated source 'WAN Primary IP'.
3. Create Loopback NAT Policy to allow access from all internal zones to the server at public IP address 10.0.93.43.

Server Access Rules
1. **WAN > DMZ** - Allow 'Any' to 'WAN Primary IP' for Service Group 'Example Web Server_services'.
Similar rules will be created from all lower security zones to the DMZ zone.

To apply these settings, click Apply. To continue, click Next.

9 The Summary page displays a summary of all the configuration you have performed in the wizard. It should show:


SonicWALL - Public Server Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Apply >
Cancel

Step 4: Public Server Configuration Summary

Review the settings for your public server.

Please review the settings below and click "Apply" to create the new objects and settings listed below. If the settings listed are not correct, simply use the "Back" button to return to the previous steps to make any changes.

Server Address Objects
1. Create 'ExampleCorpMail_private' assigned to DMZ Zone for Host 172.22.2.33.
2. Reuse 'WAN Primary IP' address object assigned to WAN Zone for 10.0.93.43.

Server Service Group Object
1. Create 'ExampleCorpMail_services' with SMTP (Send E-Mail), IMAP4 and POP3 (Retrieve E-Mail) Services.

Server NAT Policies
1. Create Server NAT Policy to rewrite packets to original destination 'WAN Primary IP' to translated destination 'ExampleCorpMail_private' for Service Group 'ExampleCorpMail_services'.
2. Create Loopback NAT Policy to allow access from all internal zones to the server at public IP address 10.0.93.43.

Server Access Rules
1. **WAN > DMZ** - Allow 'Any' to 'WAN Primary IP' for Service Group 'ExampleCorpMail_services'.
Similar rules will be created from all lower security zones to the DMZ zone.

To apply these settings, click Apply. To continue, click Next.

- Server Address Objects

The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the DMZ, the wizard binds the address object to the DMZ zone. It gives the object a name of the name you specified for the server plus "_private". If you specify an IP in the range of another zone, it will bind the address object to that zone. If you specify an IP address out of the range of any zone you have configured, the wizard will bind the address object to the LAN zone.

Because the server in the example used the default WAN IP address for the **Server Public IP Address**, the wizard states that it will use the existing WAN address object when constructing policies between the new server and the WAN. If you specify another address, the server will create an object for that address bound to the WAN zone and assign the new address object a name of the name you specified for the server plus "_public".

- Server Service Group Object

  The wizard creates a service group object for the services used by the new server. Because the server in the example is a web server, the service group includes HTTP and HTTPS. This way, you have a convenient group to refer to when creating or editing access policies for this server.

- Server NAT Policies

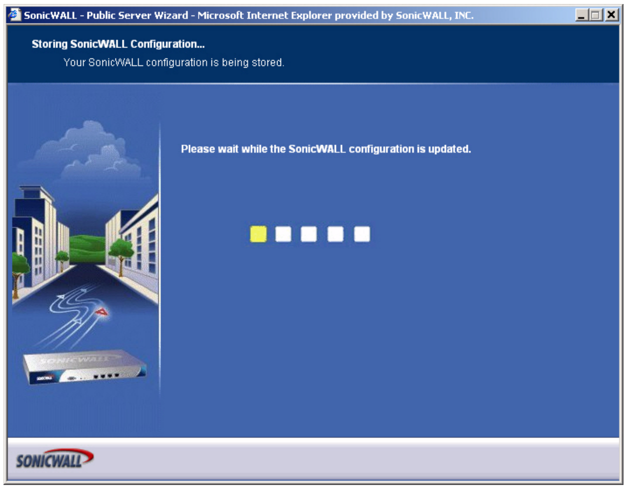
  The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. Therefore, in this example, if a packet with service type of HTTPS comes in addressed to the WAN interface (10.0.93.43), the NAT policy will translate its address to 172.22.2.44.

  The wizard also creates a Loopback NAT policy to translate HTTP and HTTPS traffic from inside your network addressed to the WAN IP address back to the address of the mail server.

- Server Access Rules

  The wizard creates an access policy allowing all mail traffic service traffic from the WAN zone to the DMZ.

10 Click **Apply** in the Public Server Configuration Summary page to complete the wizard and apply the configuration to your SonicWALL.

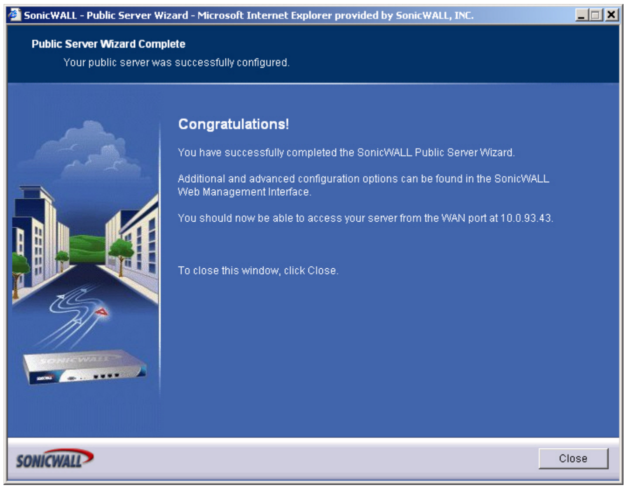

SonicWALL - Public Server Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL

Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

✓ **Tip:** *The new IP address used to access the new server, internally and externally is displayed in the* ***URL*** *field of the* ***Congratulations*** *window.*


SonicWALL - Public Server Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Public Server Wizard Complete

Your public server was successfully configured.

Congratulations!

You have successfully completed the SonicWALL Public Server Wizard.

Additional and advanced configuration options can be found in the SonicWALL Web Management Interface.

You should now be able to access your server from the WAN port at 10.0.93.43.

To close this window, click Close.

11 Click **Close** to close the wizard.

CHAPTER

50

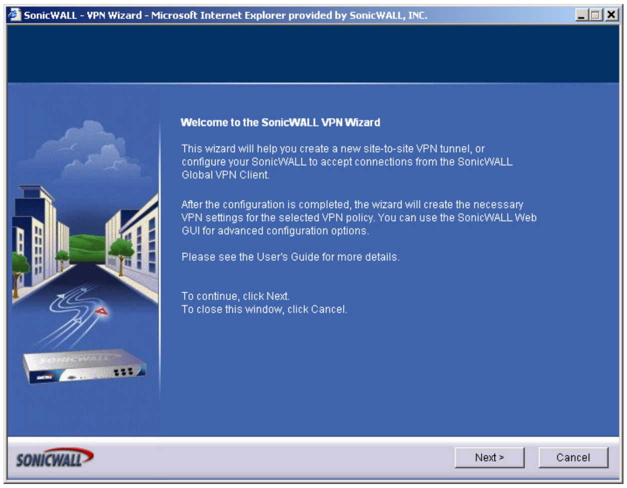
Configuring VPN Policies with the VPN Policy Wizard

Configuring GroupVPN using the VPN Policy Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN on the SonicWALL. After the configuration is completed, the wizard creates the necessary VPN settings for the selected VPN policy. You can use the SonicWALL Management Interface for optional advanced configuration options.

Using the VPN Policy Wizard

1. In the top right corner of the **VPN > Settings** page, click on **VPN Policy Wizard**.


SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Next >
Cancel

Welcome to the SonicWALL VPN Wizard

This wizard will help you create a new site-to-site VPN tunnel, or configure your SonicWALL to accept connections from the SonicWALL Global VPN Client.

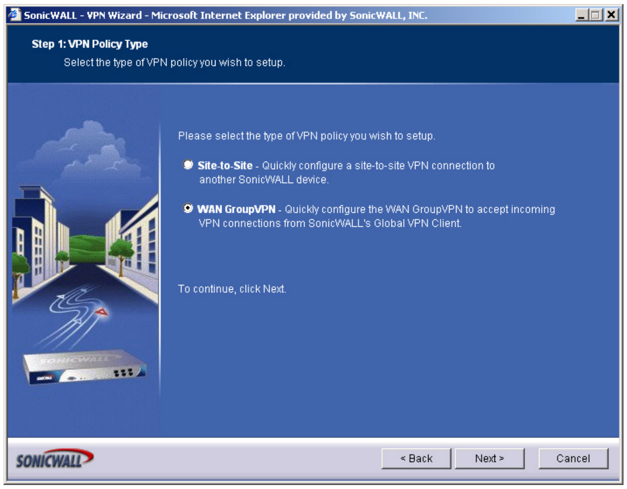
After the configuration is completed, the wizard will create the necessary VPN settings for the selected VPN policy. You can use the SonicWALL Web GUI for advanced configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

2. Click **Next**.

3. In the **VPN Policy Type** page, select **WAN GroupVPN** and click **Next.**



SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: VPN Policy Type

Select the type of VPN policy you wish to setup.

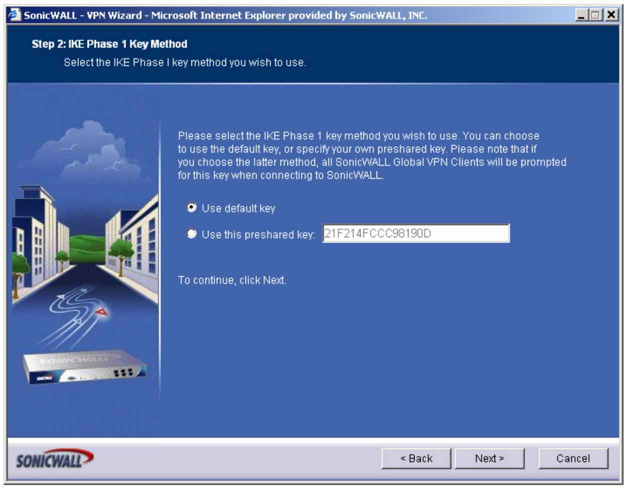
Please select the type of VPN policy you wish to setup.

○ **Site-to-Site** - Quickly configure a site-to-site VPN connection to another SonicWALL device.

● **WAN GroupVPN** - Quickly configure the WAN GroupVPN to accept incoming VPN connections from SonicWALL's Global VPN Client.

To continue, click Next.

4. In the **IKE Phase 1 Key Method** page, you select the authentication key to use for this VPN policy:



SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: IKE Phase 1 Key Method

Select the IKE Phase I key method you wish to use.

Please select the IKE Phase 1 key method you wish to use. You can choose to use the default key, or specify your own preshared key. Please note that if you choose the latter method, all SonicWALL Global VPN Clients will be prompted for this key when connecting to SonicWALL.

● Use default key

○ Use this preshared key: 21F214FCCC98190D

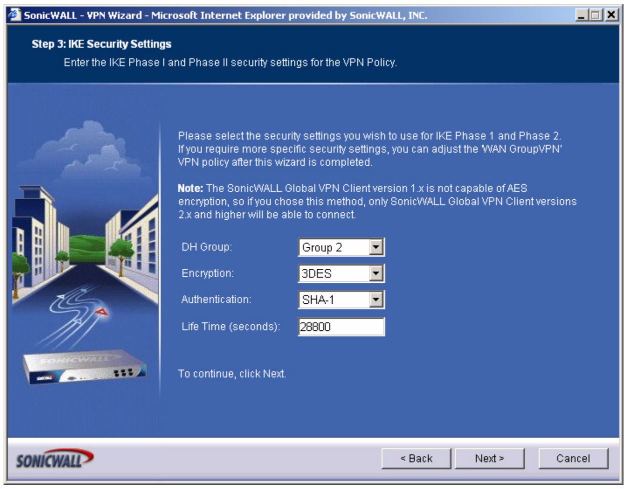
To continue, click Next.

- **Default Key**: If you choose the default key, all your Global VPN Clients and Global Security Clients will automatically use the default key generated by the SonicWALL to authenticate with the SonicWALL.
- **Use this Key**: If you choose a custom preshared key, you must distribute the key to every VPN Client because the user is prompted for this key when connecting to the SonicWALL.

Note: *If you select Use this Key, and leave the default key as the value, you must still distribute the key to your VPN clients.*

5. Click **Next.**

6. In the **IKE Security Settings** page, you select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the defaults settings.


SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
< Back
Next >
Cancel
SONICWALL

Step 3: IKE Security Settings

Enter the IKE Phase I and Phase II security settings for the VPN Policy.

Please select the security settings you wish to use for IKE Phase 1 and Phase 2. If you require more specific security settings, you can adjust the 'WAN GroupVPN' VPN policy after this wizard is completed.

Note: The SonicWALL Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWALL Global VPN Client versions 2.x and higher will be able to connect.

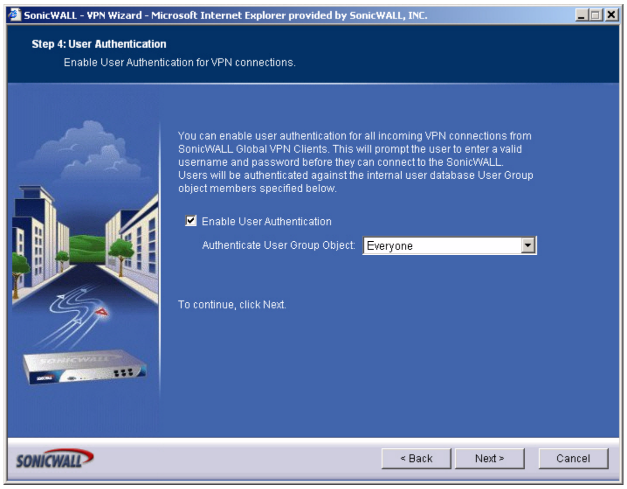
DH Group: Group 2
Encryption: 3DES
Authentication: SHA-1
Life Time (seconds): 28800

To continue, click Next.

- **DH Group**: The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose Group 1, Group 2, or Group 5. The VPN Uses this during IKE negotiation to create the key pair.
- **Encryption**: This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. DES, 3DES, AES-128, or AES-256. The VPN uses this for all data through the tunnel.
- **Authentication**: This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose MD5 or SHA-1.
- **Life Time (seconds)**: This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (28800).

Alert: *The SonicWALL Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWALL Global VPN Client versions 2.x and higher will be able to connect.*

7. Click **Next**.
8. In the **User Authentication** page, select if you want the VPN Users to be required to authenticate with the firewall when they connect. If you select **Enable User Authentication**, you must select the user group which contains the VPN users. For this example, leave **Enable User Authentication** unchecked.


SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
< Back
Next >
Cancel
SONICWALL

Step 4: User Authentication

Enable User Authentication for VPN connections.

You can enable user authentication for all incoming VPN connections from SonicWALL Global VPN Clients. This will prompt the user to enter a valid username and password before they can connect to the SonicWALL. Users will be authenticated against the internal user database User Group object members specified below.

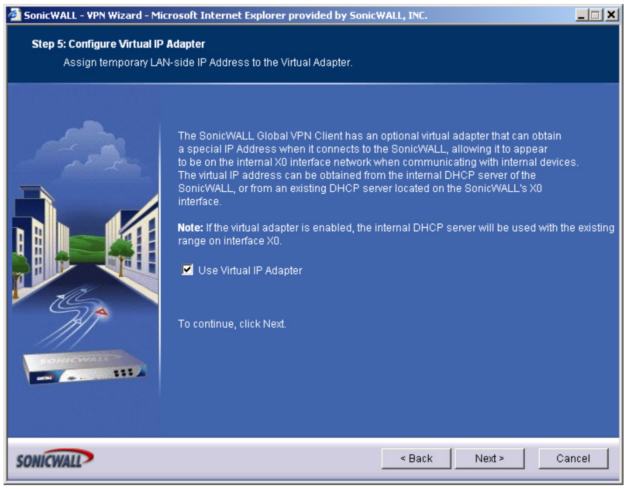
☑ Enable User Authentication

Authenticate User Group Object: Everyone

To continue, click Next.

Note: *If you enable user authentication, the users must be entered in the SonicWALL database for authentication. Users are entered into the SonicWALL database on the **Users>Local Users** page, and then added to groups in the **Users>Local Groups** page.*

9. Click **Next**.
10. In the **Configure Virtual IP Adapter** page, select whether you want to use the SonicWALL's internal DHCP server to assign each VPN client IP address from the LAN zone's IP range. Therefore, when a user connects, it appears that the user is inside the LAN. Check the **Use Virtual IP Adapter** box and click **Next**.



SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: Configure Virtual IP Adapter

Assign temporary LAN-side IP Address to the Virtual Adapter.

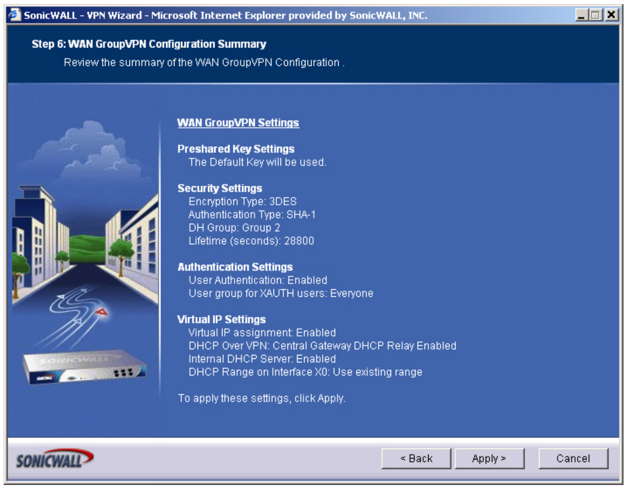
The SonicWALL Global VPN Client has an optional virtual adapter that can obtain a special IP Address when it connects to the SonicWALL, allowing it to appear to be on the internal X0 interface network when communicating with internal devices. The virtual IP address can be obtained from the internal DHCP server of the SonicWALL, or from an existing DHCP server located on the SonicWALL's X0 interface.

Note: If the virtual adapter is enabled, the internal DHCP server will be used with the existing range on interface X0.

☑ Use Virtual IP Adapter

To continue, click Next.

11. The **Configuration Summary** page details the settings that will be pushed to the SonicWALL when you apply the configuration. Click **Apply** to create your GroupVPN.



SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: WAN GroupVPN Configuration Summary

Review the summary of the WAN GroupVPN Configuration .

WAN GroupVPN Settings

Preshared Key Settings
The Default Key will be used.

Security Settings
Encryption Type: 3DES
Authentication Type: SHA-1
DH Group: Group 2
Lifetime (seconds): 28800

Authentication Settings
User Authentication: Enabled
User group for XAUTH users: Everyone

Virtual IP Settings
Virtual IP assignment: Enabled
DHCP Over VPN: Central Gateway DHCP Relay Enabled
Internal DHCP Server: Enabled
DHCP Range on Interface X0: Use existing range

To apply these settings, click Apply.

Connecting the Global VPN Clients

Remote SonicWALL Global VPN Clients install the Global VPN Client software. Once the application is installed, they use a connection wizard to setup their VPN connection. To configure the VPN connection, the client must have the following information:

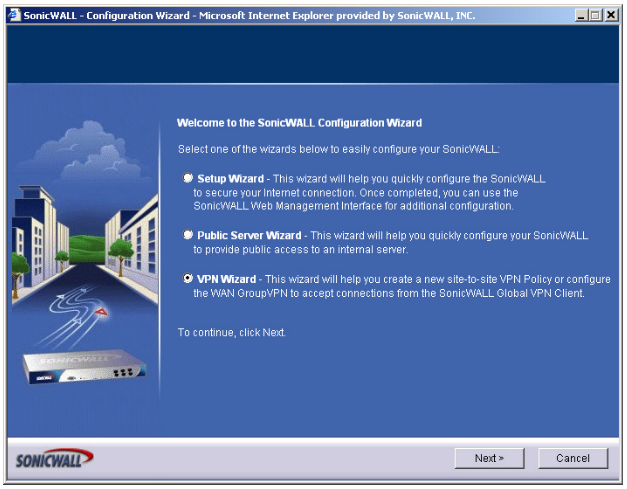
- A public IP address (or domain name) of the WAN port for your SonicWALL
- The shared secret if you selected a custom preshared secret in the VPN Wizard.
- The authentication username and password.

Configuring a Site-to-Site VPN using the VPN Wizard

You use the **VPN Policy Wizard** to create the site-to-site VPN policy.

Using the VPN Wizard to Configure Preshared Secret

1. On the **System>Status** page, click on **Wizards**.
2. In the **Welcome to the SonicWALL Configuration Wizard** page select **VPN Wizard** and click **Next**.



SonicWALL - Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Welcome to the SonicWALL Configuration Wizard

Select one of the wizards below to easily configure your SonicWALL:

○ **Setup Wizard** - This wizard will help you quickly configure the SonicWALL to secure your Internet connection. Once completed, you can use the SonicWALL Web Management Interface for additional configuration.

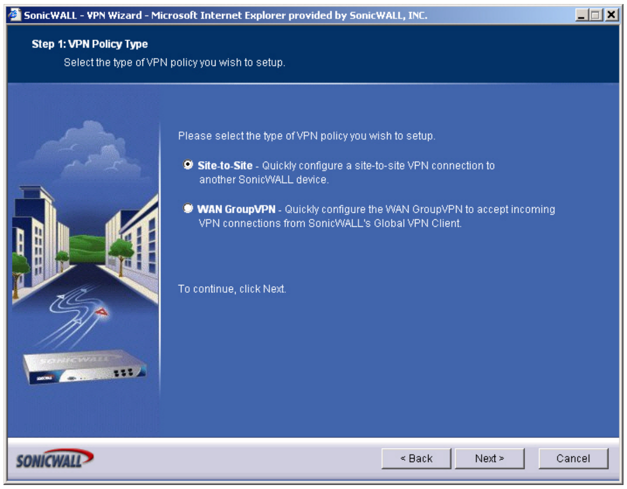
○ **Public Server Wizard** - This wizard will help you quickly configure your SonicWALL to provide public access to an internal server.

● **VPN Wizard** - This wizard will help you create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept connections from the SonicWALL Global VPN Client.

To continue, click Next.

SONICWALL
Next >
Cancel

3. In the **VPN Policy Type** page, select **Site-to-Site** and click **Next**.



SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: VPN Policy Type

Select the type of VPN policy you wish to setup.

Please select the type of VPN policy you wish to setup.

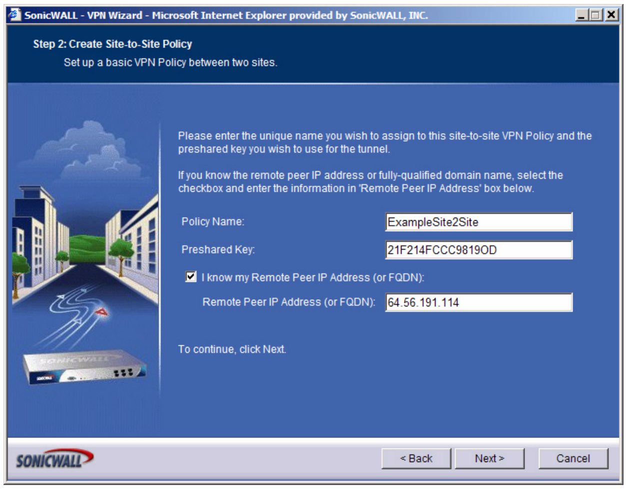
● **Site-to-Site** - Quickly configure a site-to-site VPN connection to another SonicWALL device.

○ **WAN GroupVPN** - Quickly configure the WAN GroupVPN to accept incoming VPN connections from SonicWALL's Global VPN Client.

To continue, click Next.

SONICWALL
< Back
Next >
Cancel

4. In the **Create Site-to-Site Policy** page, enter the following information:


SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 2: Create Site-to-Site Policy

Set up a basic VPN Policy between two sites.

Please enter the unique name you wish to assign to this site-to-site VPN Policy and the preshared key you wish to use for the tunnel.

If you know the remote peer IP address or fully-qualified domain name, select the checkbox and enter the information in 'Remote Peer IP Address' box below.

Policy Name: ExampleSite2Site

Preshared Key: 21F214FCCC9819OD

☑ I know my Remote Peer IP Address (or FQDN):

Remote Peer IP Address (or FQDN): 64.56.191.114

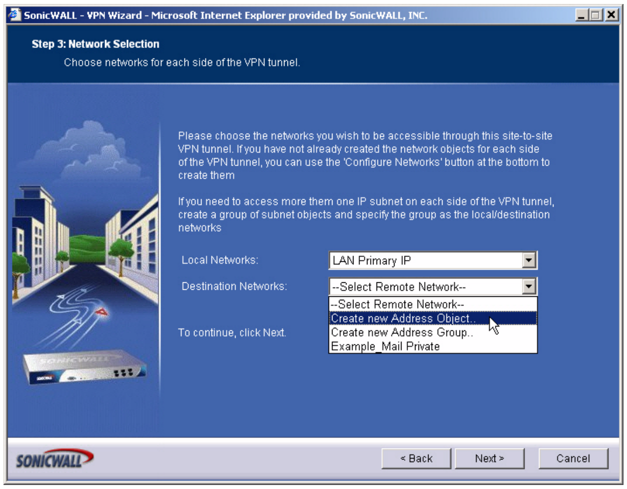
To continue, click Next.

- **Policy Name**: Enter a name you can use to refer to the policy. For example, Boston Office.
- **Preshared Key**: Enter a character string to use to authenticate traffic during IKE Phase 1 negotiation. You can use the default SonicWALL generated Preshared Key.
- **I know my Remote Peer IP Address (or FQDN)**: If you check this option, this SonicWALL can initiate the contact with the named remote peer.

  If you do not check this option, the peer must initiate contact to create a VPN tunnel. This device will use aggressive mode for IKE negotiation.

  For this example, leave the option unchecked.
- **Remote Peer IP Address (or FQDN)**: If you checked the option above, enter the IP address or Fully Qualified Domain Name (FQDN) of the remote peer (For example, *boston.yourcompany.com*).

5. Click **Next.**
6. In the **Network Selection** page, select the local and destination resources this VPN will be connecting:


SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
--Select Remote Network--
Create new Address Object..
Create new Address Group..
Example_Mail Private
SONICWALL
< Back
Next >
Cancel

Step 3: Network Selection

Choose networks for each side of the VPN tunnel.

Please choose the networks you wish to be accessible through this site-to-site VPN tunnel. If you have not already created the network objects for each side of the VPN tunnel, you can use the 'Configure Networks' button at the bottom to create them

If you need to access more them one IP subnet on each side of the VPN tunnel, create a group of subnet objects and specify the group as the local/destination networks

Local Networks: LAN Primary IP

Destination Networks: --Select Remote Network--

To continue, click Next.

- **Local Networks**: Select the local network resources protected by this SonicWALL that you are connecting with this VPN. You can select any address object or group on the device, including networks, subnets, individual servers, and interface IP addresses.

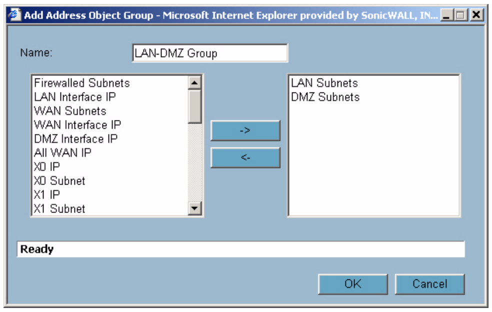
  If the object or group you want has not been created yet, select **Create Object** or **Create Group**. Create the new object or group in the dialog box that pops up. Then select the new object or group.

For this example, select **LAN Subnets**.

- **Destination Networks**: Select the network resources on the destination end of the VPN Tunnel. If the object or group does not exist, select **Create new Address Object** or **Create new Address Group**.

  For example:

  a Select **Create new Address Group**.


Add Address Object Group - Microsoft Internet Explorer provided by SonicWALL, IN...
->
<-
OK
Cancel

Name: LAN-DMZ Group

Firewalled Subnets
LAN Interface IP
WAN Subnets
WAN Interface IP
DMZ Interface IP
All WAN IP
X0 IP
X0 Subnet
X1 IP
X1 Subnet

LAN Subnets
DMZ Subnets

Ready

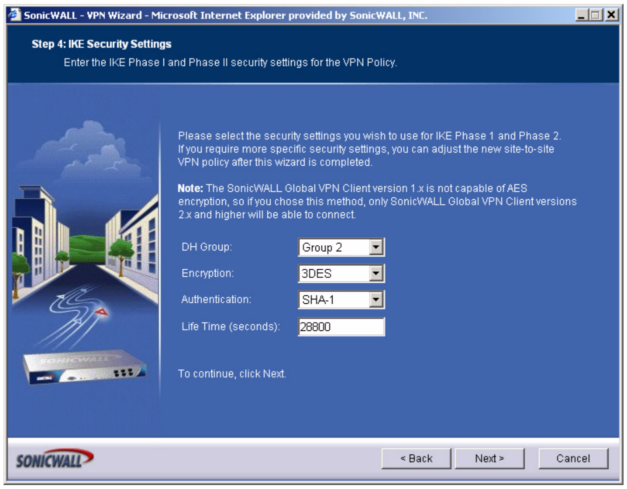
  b In the **Name** field, enter “LAN Group”.

  c In the list on the left, select **LAN Subnets** and click the **->** button.

  d Click **OK** to create the group and return to the Network Selection page.

  e In the **Destination Networks** field, select the newly created group.

7. Click **Next**.
8. In the **IKE Security Settings** page, select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the default settings.


SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 4: IKE Security Settings

Enter the IKE Phase I and Phase II security settings for the VPN Policy.

Please select the security settings you wish to use for IKE Phase 1 and Phase 2. If you require more specific security settings, you can adjust the new site-to-site VPN policy after this wizard is completed.

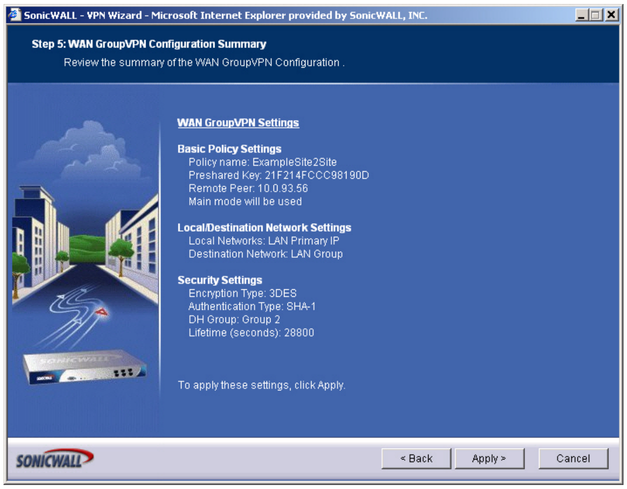
Note: The SonicWALL Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWALL Global VPN Client versions 2.x and higher will be able to connect.

DH Group: Group 2
Encryption: 3DES
Authentication: SHA-1
Life Time (seconds): 28800

To continue, click Next.

- **DH Group**: The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose Group 1, Group 2, or Group 5. The VPN Uses this during IKE negotiation to create the key pair.
- **Encryption**: This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. DES, 3DES, AES-128, or AES-256. The VPN uses this for all data through the tunnel
- **Authentication**: This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose MD5 or SHA-1.
- **Life Time (seconds)**: This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (28800).

9. The **Configuration Summary** page details the settings that will be pushed to the security appliance when you apply the configuration.


SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Apply >
Cancel

Step 5: WAN GroupVPN Configuration Summary

Review the summary of the WAN GroupVPN Configuration .

WAN GroupVPN Settings

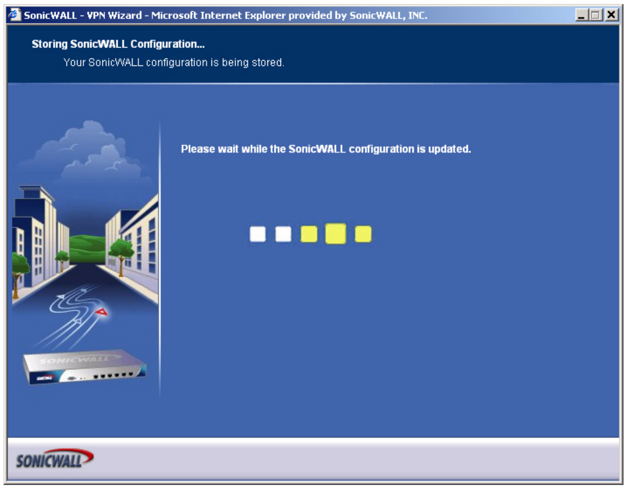
Basic Policy Settings
Policy name: ExampleSite2Site
Preshared Key: 21F214FCCC98190D
Remote Peer: 10.0.93.56
Main mode will be used

Local/Destination Network Settings
Local Networks: LAN Primary IP
Destination Network: LAN Group

Security Settings
Encryption Type: 3DES
Authentication Type: SHA-1
DH Group: Group 2
Lifetime (seconds): 28800

To apply these settings, click Apply.

10. Click **Apply** to create the VPN.


SonicWALL - VPN Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL

Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

Index

Numerics
802.11a 121
802.11g 121
A
acceptable use policy 211
access aules
    bandwidth management 134
access point IDS 130
access points
    SonicPoints 119
access rules
    adding 135
    advanced options 139
    deleting 135
    displaying traffic statistics 135
    editing 135
    enabling or disabling 135
    examples 139
    public server wizard 332
    scheduling 143
    view styles 135
    viewing 135
    zones 135
add 137
address group
    VPN policy wizard 341
address object
    VPN policy wizard 341
address objects
    about 79
    adding 85
    creating groups 85
    default 81
    host 79
    MAC address 79
    network 79
    public server wizard 331
    range 79
    types 79
administration
    administrator name and password 28
    firewall mame 27
    GMS management 31
    login security 28
    SNMP management 30
    VPN client download URL 33
    web management settings 28
advance access rules 141
advanced access rules
    drop source routed packets 142
    force inbound and outbound FTP data connections to use default port 20 142
    inactivity timeout 142
    randomize IP ID 142
    RTSP transformations 142
    stealth mode 142
    support for Oracle (SQLNet) 142
    support for Windows Messenger 142
alerts 292
    redundancy filter 292
ARP 105
    flushing cache 106
    navigating and sorting entries 105
authentication
    VPN policy wizard 337
C
certificate revocation list, see CRL
certificates
    deleting 201
    private key 200
    signing request 201
consent 246
consistent NAT 156
content filtering service 241
    activating 242
    blocked message text 245
    CFS Standard 241
CRL 200
    automatic updates 200
custom list 245
D
DF bit 186
DH group 337
    VPN policy wizard 341
DHCP
    relay mode 187
    setup wizard 309
    VPN central gateway 187
    VPN remote gateway 189
DHCP over VPN
    leases 191
DHCP server 107
    current leases 111
    dynamic ranges 108
    static entries 110
    VoIP settings 110

diagnostics
  DNS name lookup 44
  find network path 44
  packet trace 45
  ping 44
  tech report 46
  trace route 47
Diffie-Hellman, see DH group
Distributed Enforcement Architecture (DEA) 253
DNS
  configuring 77
  inherit settings dynamically 77
  specify DNS servers manually 77
  with L2TP server 194
DSL
  setup wizard 312

E

E-mail filter 251
encryption
  VPN policy wizard 337, 341

F

failure trigger level 185
filter properties 245
FIPS 41
firmware management
  automatic notification 38
  backup firmware image 40
  booting firmware 39
  export settings 38
  import settings 37
  safemode 40
  updating firmware 40
fragmented packet handling 186

G

Global VPN Clients
  VPN policy wizard 338
groups
  adding‘ 216
  users 215
guest profiles 218
guest services 217
  guest profile 218
  login status window 218
guest status 223

H

H.323 155
  transforming H.323 messages 157
hardware failover
  before configuring 228
  configuring 231
  crash detection 227
  forcing transitions 232
  how it works 227
  monitoring links 233
  status 233
  synchronize settings 231
  synchronizing firmware 233
  terminology 229

I

IDS 129
  authorizing access points 130
  rogue access points 130
IKE
  DH group 337
  phase 2 341
  VPN policy wizard 341
IKE dead peer detection 185
interface
  Ethernet settings 56
  Internet traffic statistics 52
  physical 51
interfaces
  bandwidth management 61
  configuring LAN/DMZ/OPT interfaces 54, 55
  configuring WAN interface 57
  settings 52
  transparent mode 55
intrusion detection system, see IDS
intrusion prevention service
  activating 256
  architecture 255
  deep packet inspection 254
  terminology 255
IP Helper 113
  add policy 114
ISP
  setup wizard 312

L

L2TP 193
  configurring 194
L2TP-over-IPSec 193
LAN
  setup wizard 310
Layer 2 Tunneling Protocol, see L2TP
local groups
  adding 216
local users 213
  adding 214
  editing 215
log
  alert log messages 264
  automation 297
  critical log messages 264
  debug log messages 288
  email alert addresses 297
  e-mailing logs 263
  error log messages 264
  event message priority levels 263
  exporting 263
  generating reports 299

  info log messages 274
  legacy attacks 292
  log categories 294
  mail server settings 297
  notice log messages 272
  redundancy filter 292
  view table 262
  viewing events 261
  warning log messages 267
login status window 218
logs
  priority, configuring 292
loopback policy 332

M

manage security services online 24
management interface 12
  accessing 9
  applying changes 12
  getting help 13
  logging out 13
mandatory filtered IP addresses 247
MCUs 156
multicast 151
  create a new multicast object 152
  IGMP state table 152
  multicast state table entry timeout 152
  reception of all multicast addresses 152
  require IGMP membership reports for multicast data forwarding 152
  snooping 152
mySonicWALL.com 19, 237, 256
  creating an account 20

N

NAT
  consistent 156
NAT policies 93
  comment field 96
  creatiing 97
  creating a many-to-many NAT policy 98
  creating a many-to-one NAT policy 97
  creating a one-to-one NAT policy for inbound traffic 99
  creating a one-to-one NAT policy for outbound traffic 99
  enable 96
  inbound interface 96
  inbound port address translation via one-to-one NAT policy 100
  inbound port address translation via WAN (X1) IP address 101
  navigating and sorting 94
  original destination 95
  original service 95
  original source 95
  settings 95
  translated destination 95
  translated service 95
  translated source 95
NAT policy
  loopback policy 332
  outbound interface 96
  public server wizard 332
  reflective policy 96
NAT traversal 186
network anti-virus 249
  activating 250
network settings
  setup wizard 308

O

objects
  service group 332

P

phase 2
  VPN policy wizard 341
PPPoE
  setup wizard 309
PPTP
  setup wizard 309
preshared key
  VPN policy wizard 340
PSTN 155
public server sizard
  starting 329
public server wizard 331
  access rules 332
  NAT policies 332
  server address objects 331
  server name 330
  server private IP address 330
  server t ype 330
  service group object 332

R

RADIUS
  configuring user authentication 206
  with L2TP server 194
restarting the SonicWALL security appliance 48
restrict web features 244
rogue access points 130
route policies 89
routing 87
  metric values 89
  policy based routing 89
  route advertisement 87
  route advertisement configuration 87
  route policies table 90
  route policy example 90
  static routes 87

S
SDP 124, 157
security services
  licenses 23
  manage licenses 239
  manual upgrade 25
  manual upgrade for closed environments 25
  settings 239
  summary 238
service group
  public server wizard 332
services 145
  adding custom services 147
  adding custom services group 148
  default services 146
  supported protocols 146
settings
  users 206
  VPN 161
setup wizard
  change password 308, 313, 318, 323
  change time zone 309, 313, 319, 324
  configuration summary 311, 316, 321, 326
  DHCP 326
  DHCP mode 312
  DHCP server 321
  DHCP settings 315
  LAN DHCP settings 311
  LAN settings 310, 315, 320, 325
  NAT with DHCP client 314
  NAT with PPPoE 317
  NAT with PPPoE client 320
  NAT with PPTP 322
  NAT with PPTP client 325
  static IP address with NAT enabled 307
  WAN Network mode 324
  WAN network mode 309, 314, 319
SIP 155
  media 157
  signaling 157
  transforming SIP messages 157
site-to-site VPN
  policy name 340
  VPN policy wizard 339
SonicOS Enhanced 2.5
  new features 1
SonicPoint
  provisioning profiles 120
SonicPoints 119
  IDS 129
  managing 119
SonicWALL discovery protocol, see SDP
SonicWALL registration 19
SonicWALL simple provisioning protocol, see SSPP
SonicWALL technical support 6
  options 6
SonicWALL ViewPoint 301
  activating 301
  enabling 303
SSPP 125
static IP
  setup wizard 309
status
  users 205
syslog
  adding server 296
  event redundancy rate 296
  server settings 296
syslog server 295
system
  alerts 18
  information 18
  network interfaces 22
  status 17
T
This 133
time
  NTP settings 36
  setting 36
trusted domains 244
U
user authentication
  VPN policy wizard 337
users
  acceptable use policy 211
  active sessions 205
  adding 214
  adding local groups 216
  authentication methods 206
  configuring RADIUS authentication 206
  creating local groups 215
  editing 215
  global settings 210
  groups 215
  guest accounts 219
  guest profile 218
  guest services 217
  guest status 223
  local users 213
  login status window 218
  settings 206
  SonicWALL authentication 214
  status 205
V
virtual IP adapter
  VPN policy wizard 338

VPN 161, 185
  active L2TP sessions 195
  active tunnels 164
  advanced settings 185
  CA certificates 197
  CRL 200
  DF bit 186
  DHCP leases 191
  DHCP over VPN 187
    central gateway 187
    remote gateway 189
  DHCP relay mode 187
  export client policy 170
  global security client 161
  global VPN glient 161
  GroupVPN 164
  L2TP Server 193
  L2TP-over-IPSec 193
  local certificates 200
  NAT traversal 186
  planning sheet 171
  settings 161
  site-to-site 171
  VPN policy window 172
  VPN policy wizard 335
VPN policy wizard
  authentication 337, 341
  configuration summary 342
  connecting Global VPN Clients 338
  destination networks 341
  DH group 337, 341
  encryption 337, 341
  IKE phase 1 key method 336
  IKE security settings 337, 341
  life time 341
  local networks 340
  peer IP address 340
  policy name 340
  preshared key 340
  site-to-site VPN 339
  user authentication 337
  virtual IP adapter 338
  VPN policy type 336

W

WAN
  GroupVPN 336
WAN failover 63
  caveats 63
  enabling WAN probe monitoring 66
  outbound load balancing methods 65
  setting up 64
  statistics 68
web proxy 115
  bypass proxy servers 116
  configuring 115
WEP 121
wireless
  IDS 129
  SonicPoints 119
  station status 127
wireless encryption protocol, see WEP
wireless zones 119
wizard
  setup wizard 307

Z

zone
  SonicPoints 119
  wireless 119
zones 69
  adding 73
  allow interface trust 71, 73
  enabling security services 71
  how zones work 69
  predefined 70
  security types 71
  zone settings table 72

SonicWALL,Inc.
1143 Borregas Avenue T: 408.745.9600 www.sonicwall.com
Sunnyvale,CA 94089-1306 F: 408.745.9300

© 2004 SonicWALL, Inc. SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change with out notice.

P/N 232-000427-05
Rev A 06/04